CRC Press
Taylor & Francis Group

Cyber CISO Marksmanship

Hitting the Mark in Cybersecurity Leadership

Ken Dunham, James Johnson, Joseph McComb

3 Structured for success 74

Regulatory, compliance, and insurance requirements 74
Cybersecurity frameworks 81
Communicating cyber risk 84
Designing roadmaps with balance 93

4 Defending the enterprise 101

Managing enterprise risk 101
Operations 113
Incident response 123

5 Disaster readiness planning 137

Business continuity 137
Impact assessments 141
Tabletop exercises 147
Insurance conditions and criteria 150
Legal preparedness 153
Recommendations for difficult situations 155
Contracts, SLAs, and legal enablement 159

6 Digital transformation 163

Zero-trust architecture (ZTA) 163
Cloud first adoption and migration 167

Index 183

Foreword

> “A true leader has the con dence to stand alone, the courage to make tough decisions, and the compassion to listen to the needs of others. He (or she) does not set out to be a leader, but becomes one by the equality of his (or her) actions and the integrity of his (or her) intent.”
>
> Douglas MacArthur

The only place where success comes before work is in the dictionary. In Cyber CISO Marksmanship, the authors share from their hard-fought battles the lessons they have learned over decades of time on the Cyber battle eld. Their work, which they express so thoughtfully in this book, is your path to accelerate the success you can have as a CISO.

I have long believed there are two battle elds a CISO faces daily. The external battle eld of threat actors and vulnerabilities that we see every sec ond of every day whether it is from a threat intelligence feed, an alert from the array of cybersecurity tools we have deployed, or from a risk assessment the security team performed. On this battle eld, your entire organization is engaged every second of every day. It is one where we can become weary, but we realize our strength comes from the struggle.

But there is another battle eld. It is the internal battle eld of budgets, bureaucracy, and behavior. This battle eld is lonelier. While most of the secu rity team has their aim focused on the external battle eld, it is the marksman ship of the CISO on the internal battle eld that can, in most cases, decide the fate of risk for the organizations we support. It can also determine the fate of the CISO themselves when it comes to operating with integrity.

This is not just another security book. Stories are data with a soul. Ken, James, Joe, and Jason share their stories on both battle elds so that we can learn, so our work can be more effective, and ultimately so we can succeed. They are true leaders.

Malcom Harkins
“Sharpshooter” expert,
Chief Security and Trust Of cer,
HiddenLayer.

Preface

Ken Dunham, one of the authors of this book, while working as a consultant with F100 organizations regularly performed vCISO services for organizations. In this capacity, Mr. Dunham and respected colleagues discussed gaps regularly seen in leadership, where the industry commonly missed the mark, and where leaders were commonly struggling to find support. Mr. Dunham brought together industry leaders to collaborate and establish a global community to fill this gap, so that global CISOs would no longer be alone while striving to create change in a complex and challenging role.

Beyond the standard technical and regulatory expertise, you would expect from a book of this nature, the co-authors, Ken Dunham, James Johnson, Joseph McComb, and Jason Elrod, harness the power of narrative and metaphor to inspire lasting change and drive meaningful action in the realm of executive leadership. This book offers not just advice but mentorship, drawing on the extensive experience of the co-authors to provide readers with a roadmap to leadership excellence. The authors, having climbed the ranks from the ground up, possess intimate knowledge of the challenges and triumphs at each stage of a cybersecurity professional's career. This perspective makes them uniquely equipped to guide leaders at all levels, from those taking their first steps into management to seasoned executives.

Storytelling is another unique angle used in the approach for this book. In over 30 years of leadership and consultation, Mr. Dunham has experienced storytelling as an essential part of personal relationships and connections. This powerful form of messaging has manifested itself in *Cyber CISO Marksmanship* with the wisdom and insight of four different CISO personalities and backgrounds. Within the book, our CISO Sharpshooters provide a wealth of valued inputs and information that every CISO will treasure.

This book should not be used as a substitute for the advice of a competent attorney admitted to or authorized to practice in your jurisdiction. Stories are based on true stories and experiences by authors and supporting contributors. Stories may include a compilation of collective author experiences and interpretations that are fictitious to a given individual and not relevant

Shawn Murray
Shawn Murray is President and CAO at Murray Security Services and was previously assigned to the United States Missile Defense Agency as a senior cybersecurity professional. His previous assignments included work with the US Army Cyber Command in Europe, the US Air Force, and the commercial industry in various information assurance and cybersecurity roles. He has traveled the globe performing physical and cybersecurity assessments on critical national defense and coalition programs, has prepared reports for the House Armed Services Committee, and has testified for the US Senate on small business concerns. He is the lead cyber consultant at the Pikes Peak Small Business Development Center (SBDC) and sits on the national SBDC cyber working group.

Dr. Murray has worked with SBA, the Colorado Attorney General's office, the NSA, FBI, CIA, and the US Defense and State Departments on various Cyber initiatives and has over 20 years of IT, communications, and cybersecurity experience. He has presented as a featured or keynote speaker for numerous conferences across the globe. He enjoys teaching and presenting as a guest lecturer on cybersecurity, business, and computer science courses at his Cyber Academy and for several universities. He has several industry-recognized certifications, including the C|CISO, CISSP, and CRISC. He holds several degrees including an Applied Doctorate in Computer Science with a concentration in Enterprise Information Systems.

Dr. Murray is a Distinguished Fellow at the Information Systems Security Association and was recently elected as the new President of the International Board of Directors. He is a member of ISC2, ACM, IEEE, ISACA, and the Colorado Springs World Affairs Council. He enjoys spending time traveling with his family, researching and collaborating with other professionals in cybersecurity and Cyber Law, and playing soccer in a local league in Colorado Springs.

https://www.linkedin.com/in/dr-shawn-p-murray-3a618a13/

Malcolm Harkins
Malcolm Harkins is the Chief Security and Trust Officer at HiddenLayer. In this role, he reports to the CEO and is responsible for enabling business growth through trusted infrastructure, systems, and business processes. Malcolm is also responsible for peer outreach activities to drive global improvement in understanding cyber risks best practices to manage and mitigate those risks. He is also an independent board member, advisor to several organizations, and CISO Ambassador for Reveald. He enjoys being an executive coach to CISOs and others in a wide variety of information risk roles. Key areas of focus include the ethics around technology risk, social responsibility, total cost of controls, public policy, and driving more industry accountability.

Previously Malcolm was the Chief Security and Trust Officer at Cylance. Malcolm was previously Vice President and Chief Security and Privacy Officer (CSPO) at Intel Corporation. In that role, Malcolm was responsible

for managing the risk, controls, privacy, security, and other related compliance activities for all of Intel's information assets, products, and services.

Before becoming Intel's first CSPO, he was the Chief Information Security Officer (CISO). Over Malcolm's 24 years with Intel, he also held roles in finance, procurement, and various business operations. He managed IT benchmarking initiatives and Sarbanes-Oxley compliance; was the profit and loss manager for the Flash Product Group; was the general manager of Enterprise Capabilities, responsible for the delivery and support of Intel's Finance and HR systems; and he helped create an Intel business venture focusing on e-commerce hosting in the late 1990s.

Malcolm previously taught at the CIO Institute at the UCLA Anderson School of Management and was an adjunct faculty member at Susquehanna University in 2009. In 2010, he received the RSA Conference Excellence in the Field of Security Practices Award. He was recognized by Computerworld as one of the Premier 100 Information Technology Leaders for 2012. (ISC)² recognized Malcolm in 2012 with the Information Security Leadership Award. In September 2013, Malcolm was recognized as one of the Top 10 Breakaway Leaders at the Global CISO Executive Summit. In November 2015, he received the Security Advisor Alliance Excellence in Innovation Award. In 2023, he received the Cyber Defense Magazine award for the top Chief Security Officer. He is a Fellow of the Institute for Critical Infrastructure Technology, a non-partisan think-tank providing cybersecurity to the House, Senate, and a variety of federal agencies. Malcolm is a sought-after speaker for industry events. He has authored many white papers and, in December 2012, published his first book, Managing Risk and Information Security: Protect to Enable®. He was also a contributing author to Introduction to IT Privacy, published in 2014 by the International Association of Privacy Professionals. The 2nd edition of Malcolm's book, Managing Risk and Information Security: Protect to Enable®, was published in August of 2016. Malcolm has testified before the United States Senate Committee on Commerce, Science, and Transportation on the "Promises and Perils of Emerging Technology for Cybersecurity." He has also testified at the Federal Trade Commission hearings on data security. In 2023, Malcolm was a member of a task force led by the Center for Strategic International Studies to provide strategic direction and leadership for CISA's evolving mission to protect the federal government.

Malcolm is on the board of directors for TrustMAPP, Cyvatar, and the Cyber Risk Alliance.

Malcolm received his bachelor's degree in economics from the University of California at Irvine and an MBA in finance and accounting from the University of California at Davis.

https://www.linkedin.com/in/malcolmharkins /

Acknowledgments

The authors of the book would like to thank the innumerable number of individuals who have supported us through the years enabling us to be successful throughout our career. This includes both those that we enjoyed working with and those that were difficult, pushing us to learn in different ways, and improving our character. We give thanks to all of you, for helping shape and mold us into the leaders that we are today, to be the next best person we can be today to achieve and contoday, to be the next best
person we can be today to achieve and contoday, to be the next best
person we can be today to achieve and contoday, to be the next best

After speaking with several teams, I was contacted by an employee who reported to the Chief Financial Of ce (CFO) – and came to be instrumental in moving the project forward. With most of the management team in Europe, including the Chief Executive Of cer (CEO) and CFO, having this new team member and her connections allowed us to:

- Bring the regulatory issue to executive management's attention.
- Ask for budget, resources, and executive support.
- Pull together a project team to work on compliance.
- Gain agreement that my team owned GDPR compliance.

Once these were implemented, we had about eight months to achieve com pliance. Fortunately, my US Head of Data Privacy was instrumental in driving the project forward. Over the next eight months, we collaborated with multiple teams across the enterprise, held GDPR awareness meetings to gain employee support, and hired a privacy expert in Europe to strengthen the program.

Six months after becoming compliant, we knew the project was success ful when personal data was misplaced, and the new process which included notifying the Information Commissioner's Of ce (ICO) within the required GDPR timeframes, was followed.

Sharpshooter Tips

- Learn about the organization and nd out who the in uencers are. I would not have been successful without the help of the individual directly under the CFO.
- Be accountable. If you can be physically present, do it! Being present adds credibility to the team.
- Hire and rely on competent people. My Head of US Privacy was vital in driving the project forward.
- Provide privacy training for the entire company when everyone must adhere to new or increased regulatory requirements.

Misfire

- Hiring a consulting team to identify an issue is usually helpful in achiev ing executive support. However, if your timeline is short, you may have to try other avenues or run the program in parallel. We would never have made our timelines if we had waited for that report.

Everyone follows policy, right?

As a global CISO, I managed the security aspects of the merger with another European company. Due to the time pressure to merge the two rms, I spent a good portion of time at the European headquarters, working through imple- mentation plans to merge the two security teams. The European team was small and governance-driven. In contrast, the team in North America was

large and more operationally driven. For example, the North American team ran and managed the vulnerability scanning software and submitted findings for the IT teams to remediate. In contrast, the IT team in Europe ran their own vulnerability scanning and remediated based on the findings.

In talking with the Head of Security in Europe, he reiterated that the IT team performed vulnerability scanning and remediated findings according to policy. I asked him what standards were used to harden the company workstations, and he replied that he had spent considerable time hardening their IT systems against the Center for Information Security (CIS) benchmarks. I asked him to run a compliance report from the vulnerability scanner to understand how closely the company followed the CIS benchmarks. As he pulled the report, he exclaimed, "This can't be right; our workstations are only 35% compliant with the hardening standards we agreed upon."

Sharpshooter perspectives

SSP1 It looks like the Head of Security in Europe realized that his process wasn't working. It was clever of you to ask for a compliance scan so he could see the program's effectiveness for himself rather than you saying it wasn't working. I've never seen a compliance program work where security only has oversight, and IT uses all the tools. What works is for security and IT to work together to review the benchmark controls, evaluate the gap analysis together, and agree on implementation plans. Both teams should be able to use the tools and see the results. It's best to implement the low-risk controls first, then medium, and finally, the high-risks. Controls with significant operational concerns should be thoroughly tested before implementation. I've seen cases where controls are implemented but must be backed out due to operational impact. Thankfully, the changes didn't cause significant issues since thorough backout plans were created as part of the change management process. Due to environmental constraints, some controls are not feasible, and compensating controls must be implemented as an alternative. If there is any residual risk, it should go through the risk management process, be placed into the risk register, be accepted, and periodically reviewed for future action.

SSP2 Trust, but verify comes to mind. One of the critical movers here is to have joint dashboards and reporting on a monthly reporting cycle. We use monthly operational reviewplaced into the risk regis

when we were moving away from considering this vendor. This penetration test was completed earlier in the year, revealing massive security gaps and issues, with most security issues unresolved upon retesting. I noted the dates of the test and retest, which had taken place before my previous conversation with the Director of Security.

Sharpshooter perspectives (SSP)

SSP1 This scenario is very common for SaaS suppliers. They usually haven't been in business long, and their business model is to keep prices very cheap by forgoing common security and business practices and electing to limit their risks in the terms and conditions. In this scenario, the SaaS vendor has no clear understanding of which security controls are provided by the Google Cloud Platform and which ones are their own responsibility. Through stack mapping, all major host providers, Google, Azure, and Amazon, de ne their security controls. The SaaS provider is responsible for the rest. Without these controls, this SaaS provider cannot be HIPAA compliant, and the author did the right thing by walking away and not subjecting the company to the associated risk. Since this is HIPAA-related, I'd also add a Business Associate Agreement (BAA) review to see what the SaaS provider agrees to protect for the covered entity.

SSP2 I am curious about the title of the security lead. Was the person a security architect, or were they a manager of IT that the company asked to take on the security role part-time (with no training)? The refrain of Google, Amazon, or Microsoft handling our security is too common, and a security person knows that it matters how one con gures Google, Amazon, or Microsoft. The other common refrain is "We are used by [insert name] of a big company," meaning they must be secure if a big name uses them. That is why we ask for outside con rmation, like the certi cations. From the story, I am guessing that the security lead is more of a salesperson because not knowing that a penetration test had been performed, even if the results were awful, tells if the individual is aware of the product's security.

Target grouping

The SaaS company's Director of Security was not quali ed for such a role and was not truthful about onboarding third-party services. Most security answers re ected security capabilities from their hosted cloud services provider, not provider-owned and managed security measures (big difference).

It was clear from the discussion around penetration testing that when the original ask occurred for attestations and evidence, when the Director of Security clearly stated they had not performed any such tests to date, that he was lying, as later when they shared a report to rescue a possible sales lead that was falling away. The penetration test showed that issues identi ed months prior had not been resolved, even after retesting. This revealed

clearly that the Director of Security had performed penetration testing and could not resolve critical and high vulnerabilities discovered in production that were relatively easy to remediate. He then lied about having performed any penetration testing to date because he didn't want to admit to that ugly truth.

Sharpshooter Tips

- In the cloud, you have a shared responsibility and attack surface. If you're not personally up to speed on these complexities, get someone in your wheelhouse who is, as the advent of cloud, SaaS, and other solutions is gaining speed here in 2024. Your shared risk and responsibilities in the cloud and how to navigate that from a legal and attestations perspective are critical. Doing that upfront when you have all the power in contracts, attestations, and negotiations is essential!
- SaaS salespeople who may have a "security" title or role may come off as security people when, in fact, they are salespeople. Do not be easily convinced or hear what they want you to hear. Scrutinize their experience, certifications, and background to address your security needs as you investigate security requirements for your shared responsibility.

Misfires

- Never trust a SaaS provider outright. They are often young startups who may cut corners, including using software full of critical vulnerabilities and lacking security protocols and best practices, while telling you that their data is encrypted (referring to standard cloud volume encryption), which isn't doing much, if anything, to protect your data. Ronald Regan was right when he said, "Trust, but verify," where attestations and looking under the hood are required before buying.
- The cloud has a shared security model that requires careful consideration and management from all parties throughout the lifecycle. In SaaS provisioning, the majority of control and responsibility for selecting the SaaS provider is upfront when you have the leverage and cash to require contractual SLAs and terms to meet best practices and other conditions to lower risk. Simply acquiring a service and accepting default conditions from a SaaS provider is always a foolish move as a CISO.

We've Got a backup, right?

This question oored me in the middle of an incident by an executive of the victimized company. "We've got a backup, right?" My company, which specializes in incident response and remediation, was brought in to identify and remove the threat – ransomware! Ransomware actors changed tactics around 2020 with more targeted attacks in two realms: cheap and fast for individuals

and whaling-like targeting of organizations. The bad actors also used new tactics, like ex ltration, to force huge payouts from big organizations with deep pockets (from an actor's perspective). The medium-sized organization that hired us was in the middle of the incident in which their les had been encrypted. They had no visibility of what ex ltration may or may not have occurred, and they were in a war room with their consults, discussing what to do next. Considering their options, they didn't know the quality of the backup or if they should consider paying the ransom to get their data back and become operational post-incident.

Sharpshooter perspectives

SSP1 Well, if they don't know if they have a good backup, chances are they have no plan on how and where to restore the backup. With reservation, I'd start evaluating how much the ransom is and how I'd pay it. While doing that, I am also looking for any backups and, if found, testing them to see if they are good. I'm also looking at the "integrity" of the ransomware group and the level of assurance they will not leak any ex ltrated data if I pay the ransom. Even if I pay the ransom and if, in good faith, the hacker provides the encryp tion key, there is no guarantee that the les can be decrypted and services are restored. There is always the potential that the les have been encrypted by more than one hacker organization, and if so, multiple keys will be needed, and they must be applied in the correct order.

SSP2 I wonder if the executives are well versed in the tactics and asking, "Did the attackers corrupt our backups?" That is a very legitimate question. However, if the questions are, "Do we have backups?" or "Can we restore from our backups?" then, it sounds like business continuity and disaster recovery (BCDR) has been neglected. If it is the latter set of questions, then it is likely time to ask a negotiator for the ransom and ask someone in IT to test if they can restore a backup.

Target grouping

Fortunately, the company did not suffer a massive ransomware breach or mul tiple forms of extortion. They dodged a bullet!

The incident response scene was a true crisis because leadership had not prepared. There's so much wrong from an incident response (IR) perspective. I'll start with a high-level bulleted list to summarize the critical points!

- IR planning with play/runbooks for common threats and risks, includ ing ransomware. Everyone involved in incident response should be well trained and know how to follow the play/runbooks in case an incident occurs, such as the ones above.
- Backup and restoration are a life cycle of operations that should be ongoing for all critical les and tested regularly, especially considering

the prevalence of ransomware in 2024. This process is increasingly complex with hybrid infrastructure. You'll likely have diverse backup and restoration functions and components in your overall plan that you test and validate monthly. Don't wait for an incident to discover your backups and restoration processes aren't working as expected!

- Escalation planning must exist with pre-established relationships, including legal and local authorities. These relationships are becoming more critical, especially if you're a publicly traded company in the US dealing with a material event and/or incurring losses or damages of $1 million or more.
- Ransomware readiness is its own beast – are you ready? What conditions and criteria do you have to follow to meet legal, insurance, and other requirements to consider a payout? Is it even legal in your area, because in some places it's not? If you intend to pay as a contingency, can you? Do you even know what bitcoin is, how to monetize millions in bitcoin for a bad actor, or how you may want to execute that transaction in such an event? Effective planning, thorough preparation, and creating accounts are necessary for speed and readiness if you're hit with ransomware.
- Data integrity matters. What controls do you have in place to ensure that, if you're performing recovery following an incident or potentially receiving data back from bad actors, you don't unknowingly end up with compromised, injected, or weaponized data? Golden images, approved software, hash lists, and similar solutions are required to assure data integrity.

Sharpshooter Tips

- Identify the organization's top threats and risks and ensure you're prepared to identify, respond to, and proactively reduce risk against each. As the CISO, this is one of your essential responsibilities. Ensure your highest-value assets have the best security measures to protect you from the most significant risks.
- Backup and recovery are often shared responsibilities between IT and security, requiring complete tests to ensure operational effectiveness and readiness. A BCDR program requires business units to identify roles and responsibilities (RACI) and regularly validate that essential backup and recovery functions are operational. Don't wait for a significant security incident like ransomware to discover your BCDR isn't functional as expected. You must commit to training your team, operationalizing, and testing the BCDR to confirm you're ready for a disaster.

Misfire

- "If you fail to plan, you are planning to fail" – Benjamin Franklin

We Don't have any participants from the EU

As I helped a group of nonprofit volunteers plan a regional cybersecurity conference, the discussion about privacy came up about the GDPR and how it might apply to registered participants. GDPR was a hot topic in the news regarding the privacy rights of individuals in the European Union. The volunteer was implying by the question that GDPR did not apply to us because our conference was in the US, and we didn't know of any European participants in the past. We needed to decide what was legal and wise to protect the data of participants registering for the conference. We also needed to determine how to manage and archive their data and the legality of sharing their information with sponsors who paid for it as part of their package.

Sharpshooter perspectives

SSP1 GDPR is irrelevant here since this conference is in the United States, and you are not conducting business in the EU. What is relevant is that you protect participant data per the applicable state privacy laws. Start by telling participants what data you collect, how their data will be used, how their data will not be used, and then do what you say. Strongly consider an "opt-in" clause where participants choose whether their PII is shared with the vendors. If they don't "opt-in," none of the vendors get the participant's PII. I'd also include a statement that they authorize the conference to notify them of the same conference in future years by registering.

SSP2 Ironically, the data protection question is being argued at a cybersecurity conference. It reminds me of a vice president who argued that we did not need to protect people's credit card data because most people would only be liable for $50. Besides, if their data were stolen, we shouldn't notify them because we wouldn't know if it would be used. GDPR can be invoked for anyone who is an EU citizen. As the prior Sharpshooter stated, the better course of action is to consider an "opt-in" clause. Define the rules for what type of data you collect and put in rules for how it is used.

Target grouping

Just as seen in our Sharpshooters Perspectives, there was a varied understanding of the implications of GDPR and how to navigate the privacy requirements of conference registrations wisely. The accurate answer is that any European Union (EU) citizen is protected under GDPR law for any company doing business in the EU. Suppose an EU citizen attends a conference or signs up and discloses their data during registration. In that case, the organization is responsible for and accountable for securing and protecting the individual's personal information. However, because the conference is in the US and the company is not doing business in the EU, it is likely not subject to GDPR (no legal jurisdiction). Regardless, the organization may be subject to local, state,

federal, national, and other laws and regulations similar to GDPR. Forrest Gump was right when he said, “Life is like a box of chocolates; you never know what you’re gonna get.” Consult an attorney for legal advice speci c to your business and location. CISOs would be wise to universalize company privacy to GDPR-like standards for uni cation and ease of global administration, especially for business units with nancial and regulatory requirements.

Sharpshooter Tip

- Universal privacy wisdom is relatively easy to achieve. GDPR attempts to regulate what should be common sense in some regards (this could be debated) in collecting, managing, removing, and performing lifecycle management of data willfully disclosed by someone. We are compliant if we afford these privacy rights to everyone, ensuring we’ve met local, state, federal, national, and GDPR laws. Usually, this rolls up to the point that if you’re performing GDPR-compliant practices, you probably comply with all other similar privacy laws. Consult with your legal counsel to ensure compliance.

Misfire

- Never make decisions based upon the “opinions” of others, who are often misinformed. If you have doubts, consult with legal counsel to understand the law and determine how privacy, contracts, and legal matters apply to you in various situations.

CYBERSECURITY FRAMEWORKS

As a CISO, have you ever faced challenges aligning priorities with your staff, advancing speci c overarching goals as a team, and achieving uni cation? Cybersecurity frameworks not only provide the required structure but can also remove the people and politics angle, where you focus on the process instead of personalities! This structure is very bene cial when dealing with turf wars, egos, and cultural challenges. Frameworks can also help you meet speci c standards that qualify you for insurance and, in some cases, lower premiums.

Embracing cybersecurity frameworks can begin with understanding “WHAT” should be included in a SecOps program, such as the NIST Cybersecurity Framework (NIST CSF) with approximately 100 controls. Start by learning the process and conducting a self-assessment, then have a third-party audit to ensure integrity, further re ne your approach, and strengthen your team’s capabilities. Once the initial framework is operational, consider upgrading to the more extensive and comprehensive NIST 800-53 or a similar cybersecurity framework. This upgraded framework should not only outline the necessary components of the program but also detail how these

components are achieved. Additionally, it should assess the maturity of operations through process and documentation, measured against the international Capability Maturity Model Integration (CMMI) model. This will allow for the baselining and maturation of operations based on business objectives, key performance indicators (KPIs), and various metrics and goals.

I need a NIST CSF assessment completed in dozens of countries in 2 months or less

When running a global cybersecurity framework consulting practice for F100, a client onboarded and asked for a baseline of operations to the NIST CSF within 2 months. Completing an extensive assessment within a month is feasible if the client can ensure timely participation and flexible availability of interviewees, prompt provision of requested documents, and regular meetings. This will allow sufficient time for data collection, interviews, analysis, and reporting. The client then stated their operations took place in dozens of countries – and yes, they wanted it all completed in 60 days. The desired outcome was establishing baseline operations, securing management's commitment to adopting a framework-driven approach, and developing a roadmap for maturing SecOps.

Sharpshooter perspectives

SSP1 My first question would be, "Does the CSF apply equally to all operations, or will there be a difference in the framework tiers: Partial, Risk Informed, Repeatable, or Adaptive?" The expected framework tiers must be established before a gap assessment can be completed. Second, I would ask if specific business units are at higher risk than others and suggest increasing emphasis on completing those assessments first. Third, I'd approach this as a remote assignment for most, only having boots on the ground for the highest-risk areas. Fourth, I'd ascertain if there are F100 employees with cybersecurity knowledge and foreign language skills and then map them to the number of assessments that must be performed in that language to determine if enough resources are available. If there is a shortage, I would request the client provide translators. From there, I'd create a quick proposal, including an implementation plan and costs, to understand their interest in completing this in 60 days.

SSP2 I would determine how invested the company is in this project. If this directive comes from the CEO, emphasizing to all units the priority of completing this baseline and indicating that penalties will be imposed on teams that do not participate, the project becomes possible. In this scenario, a project plan with allocated resources can be developed. However, if this initiative is not driven from the top, it will unlikely be completed within 60 days.

Target grouping

The project was aggressively managed across multiple geographic regions with various languages, and operational challenges unique to each area. We completed it within 60 days and followed up with additional work speci c to alignment, consumption, and next steps. To no surprise to the author, the client became very dif cult, critical, and divisive, bringing the project to a crawl. The stalled long-term adoption of a framework-driven practice quickly became evident as we better understood the organization's negative culture and top-down leadership.

One Sharpshooter accurately discussed starting in areas of highest risk or areas of priority. As a CISO, why would you begin with a challenging project with such an aggressive timeline? Was this to assert authority and try to make your staff care? Does that build motivation and team building and get them behind a framework-driven operation? No. It will likely make them resent a big push, resulting in nothing but busy work and "ammo" for the big boss to use against others and an erosion of trust. Trust is destroyed, and leadership is weaponized within the framework if utilized in this way.

Turning back to what made the project work, here are a few takeaways:

- Reiterating that the client must have high commitment and availability of resources during such a tight window. If someone was on vacation for 2 weeks, how can we stage interviews, follow-up inspection of docu ments, and other activities related to the assessment? Daily operations were established to identify risks and manage them accordingly.
- High-trust relationships, which resulted from daily operations, were essential. We worked hard to be dependable team players – responsible, professional, and agile – all striving for successful outcomes. We also connected personally, which paid off in spades when stressful situations occurred later. Trusted insiders shared with us and partnered toward outcomes to help us turn the corner with the toxic leadership above.
- Organized roles and responsibilities into highly detailed groups, broken into geographical language and technical components and mapped to dependencies. This information resulted in successfully scheduling criti cal interviews and other activities required for the assessment.
- We focused on establishing a culture of the CSF as a baseline of truth, "good, bad, or ugly," with no shame in whatever the outcome so that we could move toward maturity. This positive culture was later under- mined by toxic senior leadership with weaponized motives. We gained the respect and trust of leaders during the assessment, but senior lead ers destroyed them during the reporting and consumption phase of the assessment.
- NIST CSF is just the beginning; it establishes "WHAT" is to be in your SecOps program without the more signi cant "HOW" measured in NIST 800-53 and other frameworks. It is destroyed them during the reporting a

The obvious question on the table was: How could I succeed where others had failed?

The first few weeks were a whirlwind of meetings, reports, and assessments. I dove into the records of previous years' security failures to understand the root causes. It didn't take long to uncover the first major issue: a glaring lack of understanding of the company's core assets. The "crown jewels," as they are often referred to in cybersecurity parlance, were not clearly identified, leaving the company's most valuable information under-protected.

As I delved deeper, another revelation came to light. The majority of the cybersecurity budget and effort were channeled into protecting systems and data that, while important, were not critical to the company's survival or competitive edge.

Sharpshooter perspectives

SSP1 The classic cybersecurity story – follow the data and the money, and hopefully, the money is following the critical data. Great job on your part for identifying that was not the case. It sounds like a case where you may have to tear down the complete protection strategy and rebuild from the ground up. Create your plan, communicate it clearly, secure buy-in from key stakeholders, educate those previously involved and who missed the critical assets, implement the plan, and measure the effectiveness of its implementation.

SSP2 Moving from symptoms to the root cause is always a Sharpshooter's objective. The author has excellent insight and experience as a leader to realize and listen to the company's history, leading to identifying current challenges and core needs. A transformation is needed, but is it cultural, technical, procedural, operational, or all of the above?

I heard the term "patchwork" in relation to threat and vulnerability management (TVM), which I interpreted as fragmented, incomplete, and indicative of an immature TVM lifecycle – a situation all too common in many organizations. This patchwork often leads to higher risk exposure throughout the TVM lifecycle, with vulnerabilities and nested exposures remaining unseen and unmanaged for extended periods, potentially resulting in breaches over time.

I also noticed a lack of understanding of identifying "crown jewels." Gathering stakeholders for a 1- to 2-hour session can determine these critical assets quickly. During this meeting, we use a whiteboard to:

1. List our high-value assets (no wrong answers here).
2. Discuss how these assets are protected.
3. Evaluate the strength or weakness of defenses for each asset.

We then prioritize these assets, discussing the "why" factor related to risk, clarifying impact and likelihood, and assessing the specific risks to the company. This exercise often leads to spontaneous discussions around key risk areas such as operational downtime, breach/disclosure/reputational risks, and IP loss.

This process is an excellent starting point for fostering cultural change, enhancing transparency, and shifting the focus to risk management rather than merely addressing patching and security engineering issues.

Lastly, you need senior management that balances tactical, operational, and strategic leadership. This plan must include a roadmap and ongoing maintenance and support. Your competitive business plan is evident as part of this, with security, brand, and other elements as core components.

SSP31 was put into a similar situation as a longtime Information Security Manager. Management hired a new CISO, who started in the right direction by stating that they could prioritize risk management by working to protect the company's critical assets. I raised my hand and said no one has de ned a list of critical assets, but I can help put it together. The CISO ignored me because I was lower on the management chain. He said the DBAs would know where the critical data was and then tasked them with compiling the list. The DBAs then delegated the task back to me.

I ended up creating the list but received little credit! This experience taught me the importance of listening to different teams over the years and gather ing information about the types of data stored in each system. Sometimes, the crusty technology person who has been with the company for a while can provide valuable insights into what each system contains.

Target grouping

We spend a lot of time working on "how" to protect our organizations, but we often spend less time than we should on the "what" or "why" of that equation. In this instance, it was a classic case of misdirected priorities, which started to explain the ease with which cyber attackers had previously pen etrated the company's defenses.

I proposed conducting a BIA focused on security and privacy. This assess ment would help identify the core assets and provide a clear picture of the potential impacts of various cyber threats. It was an approach that hadn't been tried before in the company because there was a false belief that "business" and "security" were somehow separate. While some executives were hesitant, the memory of the previous year's failures led them to give the green light.

The BIA process was thorough and eye-opening, and the results were shocking yet unsurprising: roughly 80% of the cybersecurity program's resources were focused on protecting the 20% of essentially non-critical assets. The actual "crown jewels" were left almost bare, exposed to any threat actor savvy enough to spot the opportunity.

Using the BIA, we could paint a clear picture of resource misallocation, and the executive team could see the gaps in the organization's defense as plainly as holes in a block of Swiss cheese.

The solution was as elegant as it was effective: apply the Pareto Principle (80/20 rule) by reallocating resources to ensure that most of the cybersecurity budget and efforts were dedicated to protecting the "crown jewels." It was

a strategic pivot that required reshuf ing priorities, reallocating funds, and, most importantly, changing the company culture around cybersecurity.

Implementing the new strategy was a massive undertaking. Old security protocols with years of entrenchment were overhauled, and new defenses were put in place with the correct focus. Training programs were revamped to ensure that every team member was aligned with the latest priorities, and some asset-speci c solutions were deployed to strengthen the security posture of hyper-critical assets.

The transformation was not immediate, but the results began to show over the next few months.

uphold the law revealed their non-compliance and desire to force you into an unlawful situation. I am concerned this is a verbal conversation. When legal matters arise at work, I, with discretion, always follow up sparingly on such situations with documentation over email with a structure such as:

1. Thank you for your time.
2. Here is what I understood and/or Action items.
3. Please correct me if I didn't understand this correctly.

Here is an example email:

Form 5.1: Example Email to Superior
Verifying Concerning Direction

Subject: Follow-up on our Recent Conversation

Dear [Superior's Name],

I hope this email finds you well. I wanted to take a moment to request further clarification regarding our conversation earlier today to ensure I understand your instructions correctly.

During our verbal conversation earlier today, you asked me to [Describe the illegal activity your boss asked you to do], and you provided some context for why you believe this action is necessary. However, I want to confirm that my understanding is accurate and seek additional clarity on the following points:

1. [Specify the key points and details you discussed with your boss regarding the illegal activity.]
2. [Highlight any potential legal and ethical concerns that you raised during the conversation.]
3. [If there are any potential consequences or risks associated with the requested action, mention them.]

I would like to reiterate that I take our conversations seriously and want to ensure that I am following your instructions accurately. If I have misunderstood any aspect of our conversation or if you can provide further guidance or clarification on this matter, please let me know.

I appreciate your time and attention to this matter and look forward to your response. Please advise on the best course of action moving forward, as I want to ensure compliance with all applicable laws and regulations while carrying out my responsibilities.

Thank you for your understanding and support in this regard.

Sincerely,

[Your Name]

This email is an important way to document your understanding and a great way to shift liability to the other individual. They must take action to correct or document what they are saying verbally to avoid plausible deniability – especially for a supervisor asking you to perform unlawful acts. The problem is this action may raise their hackles and cause them to come after you. Going to HR may also do the same, so proceed cautiously, but do not break the law and hold fast to your convictions. When informing your direct boss, did you concisely record and document this in writing? Such sensitive matters profes sionally require sensitive handling and documentation, as described above.

SSP3 Was this considered a success? You didn't break the law and held your ground. It wasn't fun, but you navigated it and appeared to have the support of your supervisor. I would count that as a success in the face of an of ce bully attempting to cut corners by asking you to violate the law. How you de ne success in this scenario matters! How did your boss react to this, and did they coach you?

SSP4 The context of the DoE combined with "non-approved" personnel sent off immediate red ags for me as a specialist in counterintelligence, nation-state threats, and all-to-often insider threats of a contractor or individual that led to a breach.

SSP5 I hope your boss had your back on this. Having worked in the government, I have seen the same behavior, which makes me angry. I want to hear more of the story.

Target grouping

The Director of Security did provide access, and the foreign state accessed the sensitive area. Personnel action was taken against the Director, and he got early retirement. A few months later, I was promoted to headquarters. I consider the outcome of this situation a win, knowing that I was following my principle of always doing what is lawful, moral, and ethical.

Since all access is reviewed independently monthly, it wasn't long before it was questioned, and I was called upon to explain why access was provided. I took my documentation with me and explained everything that happened. While I was not directly involved, reports had to be written and issued at multiple levels within the government. During the whole investigation process, my boss had my back and provided valuable coaching. I also had support from the entire Computer and Information Security organization.

Sharpshooter Tips

- Have a predetermined set of principles and morals that you use to make decisions. These will determine the answer to dif cult situations before you face them.
- Adopt a "Yes and" mindset instead of a "No or But." You can deliver the same information, but the outcome will be entirely different based on how you communicate it.

Misfires

- Being insubordinate even when you are right has the potential for negative consequences.
- Bullies will come after you seeking more power and can be embittered, insecure, and want to push you down. You'll need trusted colleagues, managers, and political power to navigate such threats.

CONTRACTS, SLAs, AND LEGAL ENABLEMENT

We signed what?!

Cybersecurity Manager: "Hey, boss. We've got a call from an angry vendor who says they won't support us because we blocked that remote control app."

CISO: "The unsupported, exploitable, non-monitored, remote control app that resembles malware?"

Cybersecurity Manager: "Yeah. That one."

CISO: "Tell them I don't care, and then tell them to use the enterprise-supported one that is fully compliant and secure."

Cybersecurity Manager: "I think you should take this one. They refuse to use any solution other than the old app, and their lawyer tells me we are in breach of contract."

CISO: {sigh}

I really, really wish that wasn't an actual conversation I had, but it was. After getting off the phone with a major supplier of support for critical systems in my organization, I had the team pull up the support contract in question, and sure as the sun rises, the organization had signed a contract 8 years prior that specifically called out a remote controlled application that had some severe security issues. In addition, the contract specified we had a duty to pay them not only the regular fees but additional damages should we intentionally obstruct and prevent them from providing said support. I was stunned and mortified at the same time. We were contractually obligated to either pay extra for a needed service that we wouldn't receive or have to open up a known and exploitable application to the internet and take our chances.

Sharpshooter perspectives

SSP1 This is a horror story waiting to happen. Surely, this contract isn't perpetually open-ended and must be renewed periodically and hopefully annually. Upon renewal, I'd force the use of a secure tool. If it is an extended time before the renewal, I would get GC involved to help explain to the vendor that while meeting contractual requirements is essential, it doesn't automatically absolve a third party from potential liability, including cybersecurity

breaches. The vendor needs to formally understand that if they insist on a known unsecure solution to provide support, they will be held liable for any breach associated with the solution.

SSP2 Legal matters are often more about posturing than the law or what is right or just! Don't allow yourself to be bullied or threatened by another. Roosevelt said, "Speak softly and carry a big stick." This advice is the best recommendation I can give when dealing with such matters, embracing as well-rounded and experienced legal counsel as possible to understand all your options for the entire lifecycle of the immediate and long-term relationships and how to navigate the business relationship wisely. Ugly partners must be held accountable and will eventually reap what they sew. Your goal is to minimize the damage, and if you fail, fail quickly, move on, and learn from that mistake to avoid repeating it in the future before onboarding a vendor in the future of a similar nature.

SSP3 Given the organization's size, it sounds like a legal department should be on the company's side. I would start with them, outline the current contractual issues, and find out how much liability the vendor carries. I have been in this situation multiple times, and sometimes, it takes years to sort out until the contract expires. In the current common language environment for liability for security breaches, vendors find it harder to argue that controls should not be put into the contract.

Target grouping

This issue is, unfortunately, not uncommon. Many times, legacy contracts that have seen multiple renewal cycles often contain clauses or aspects that are either no longer applicable or downright wrong in the current environment. This case was one of those. This service provider was quite large and had an operational model requiring their employees to use their internal processes. This was linked to their employee training and business model – a rational enough reason but not something that made much sense. We were a "legacy" customer in their mind and had everything good and bad that came along with that.

After reviewing the contract and situation with the legal team in my organization, I got on the phone with our sales rep, their leadership, and their contract/legal team. They were 100% right in the black-and-white letter of the contract. We were indeed beholden to the specific technology listed there and the potential financial disincentives associated with interfering with that method. However, quite a few items were buried and missing in the same contract, which provided us with some leverage we could use. A lot can change in 8 years. Whereas we may have been "locked" into using a specific technology to ensure their ability to achieve the SLAs in the contract, we maintained control over where our data could be accessed and the accounting of the access that happened. The service organization had adjusted to an offshoring model outside the initially agreed scope a few

years prior. At the time of the original contract, it was noted that none of the support team was outside of the United States, and that proved to be material enough change for us to have a more “productive” conversation with the vendor.

After explaining how they had missed producing adequate accounting of the access to our systems and the location of the resources performing that access, I noted that could not only be a breach of terms in the same contract they were trying to hold us to but had also kicked off an investigation into the third-party risk of continuing with them as a vendor after the current term that was set to expire in 12 months. Needless to say, a few more options became available, allowing us to start bridging the gap between us.

After several more meetings, we landed on a third option, which was different from our recommended solution. Still, one that had a sufficient level of security controls and auditability to satisfy the technical risk concerns my team had. This modern option was their current option with other organizations, but additional licensing costs were associated with its use and required updates to the systems being supported. The price difference was insignificant, so we agreed to pay the delta, and they decided to switch away from the old platform they had drawn the hard line on using. This third option became an alternate standard at our company because of the level of industry adoption, so it was a win–win in some sense.

I do have to point out that we got lucky a bit in this. The fact of the matter was that if we hadn’t found weak points in the original language, it would have been a more painful and risky situation. It probably would have been a much more expensive solution as well. Because of this near miss, we prioritized creating an up-to-date Security Risk Addendum for all future contracts that would include the current requirements and clauses to ensure something like this didn’t happen again. This addendum was added to every renewal negotiation and new vendor contracts, regardless of where they were instantiated in the organization. As renewals came up over the next few years, I was amazed and shocked at how many other places we were contractually obligated to allow risky situations. I frequently encountered new vendors who insisted that “no one else makes us sign this,” necessitating numerous conversations to ensure we stayed on the right path.

Sharpshooter Tips

- The best time to have rational security controls is at the beginning of any third-party relationship. The second best time is at renewals. The third best is implementing them ad hoc whenever issues are discovered.
- Don’t ever take a vendor’s or partner’s word for it when it can negatively impact your organization’s risk posture. If something doesn’t seem right, research and fight for the right thing. It isn’t always easy, and sometimes it takes a little luck, but you are accountable for holding the line and fighting those fights.

- Consider annual capability assessments to validate that the third-party tools or organizations still provide the best value.

Misfire

- Never just “let it ride” when contract renewals come up. Change is the one constant in life, which is never in just one place. Make sure what you are signing today is relevant for today and not 8+ years ago. The issue should have been caught well before the time it did.

Chapter 6

Digital transformation

Cybersecurity must evolve alongside digital advancements. As technology grows more complex, so too should our defense mechanisms. The imperative is clear: adapt quickly or risk obsolescence. CISOs must anticipate emerging threats and adapt their strategies proactively. Success in cybersecurity transformation hinges on adopting new mindsets and tools and fostering a relentless pursuit of knowledge, all while maintaining foundational principles. It requires readiness to explore beyond the familiar and identify potential threats early. The effective CISO knows cybersecurity is about new technologies and nurturing mindsets to evolve with the changing digital landscape. This chapter explores the necessity of cybersecurity transformation in the face of advancing digital technologies. It delves into the importance of adapting defense strategies, fostering a culture of continuous learning, and the critical role of mindset in navigating the evolving cybersecurity landscape.

ZERO-TRUST ARCHITECTURE (ZTA)

Who do you trust?

I stared at the flickering monitor. Another data breach had occurred, and another hospital scrambled to contain the damage. Patient records were exposed, and lives were potentially at risk. It was a familiar scene, a recurring nightmare in healthcare cybersecurity.

The industry relied on a fortress mentality – a digital version of Fort Knox. Once a doctor, nurse, admin, or even a volunteer was “in” the system, access was more or less wide open. It was a system built on trust, a trust that had been repeatedly shattered.

I quietly shut my laptop. Our organization wasn’t that much better, and this model wasn’t working. Who should have access to a patient’s X-rays? An oncologist, yes. A billing clerk, definitely not. However, the current system granted access based on roles and broad strokes that painted a blurry picture. We needed something granular that mirrored the ever-changing needs of a hospital environment. “Identity has always been the security perimeter,” I

DOI: 10.1201/9781032720500-7

repeated. It wasn't about walls but who got the key and for how long. The default trust of legacy systems wasn't working.

As I pondered this, my phone buzzed, and the message indicator light blinked. Getting a text is not uncommon, but the time of night and the coincidence of timing gave it more urgency than I would typically have assigned it. The message read, "We have live connections with Company X that were just breached, and the service account assigned to them is actively being used."

Sharpshooter perspectives (SSP)

SSP1 Connections to third parties have always been one of my most significant concerns because, essentially, my network and systems accept the security posture of the third party over which I have little to no control. If you are forced into a third-party connection, here are some must-have controls under the access restriction category.

1. Limit access to only what is necessary. For example, if the third party only needs access to one application, lock them down to that application.
2. Enforce named accounts and use strong authentication methods such as MFA.
3. If access is only needed occasionally, keep access turned off until needed.
4. Frequently audit to ensure that access permissions are still needed and valid and that accounts are used only for their intended purpose.

SSP2 Securing medical environments is inherently complex due to several factors. These include the involvement of numerous stakeholders with diverse requirements and needs, a culture where security has often been overlooked, and the presence of a massive amount of Internet of Things (IoT) devices. Many of these devices have little to no security or are grossly insecure, making them easy targets for exploitation. This results in an enormous attack surface for the entire network. A significant challenge we face in 2024 is securing the most complex cyber assets in human history. This includes legacy computing, new cloud computing, and intricate hybrid infrastructures scaled across global networks. This task is unprecedented in complexity, often involving dozens of providers, thousands of applications, and countless IoT devices, with innumerable objects, people, and data constantly moving. Are you overwhelmed yet trying to secure all of this? Zero-Trust Architecture (ZTA) and embracing newer technologies and transformative solutions like software-defined networking (SDN) enable segmentation, isolation, and cloud security controls. When properly configured and managed, these technologies provide excellent granular security controls beyond the legacy controls in traditional computing

environments. When ZTA is appropriately designed and supplemented with advanced security controls, complex environments like those in the medical field can achieve identity access management, data security controls, and other requirements necessary for adequate security. This security level is impossible with traditional tools, techniques, and procedures. If you haven't transitioned from legacy computing yet, it is imperative to do so, as the evolving technology, architecture, and global realities of 2024 necessitate this transformation.

SSP3 Every environment I have ever been in had access control issues. The first access management project I was involved in aimed to "provide employees with the right access at the right time." Most access control projects are not implemented because of the cost of hiring personnel to maintain the systems and processes. We have solutions for access control, including vendor access, and the gap we always face is for people to manage the systems. The first step is to understand who governs access control. If governance is within the IT operations or service desk teams, the strategy will be to provide access to reduce calls, not security risk. This strategy leads to over-permission. The next piece to understand is whether the executives support an access control project. If management always bows to doctors or other employees, sadly, it will probably take an incident to gain support for an access control project. Hopefully, both areas will be covered in this story so that suitable controls can be implemented.

Target grouping

Legacy systems typically rely on macro controls, like having a single security guard oversee an entire hospital. In contrast, ZTA employs micro controls, effectively placing a security guard at the door of every room. This approach creates a finer, more adaptable security mesh that can adjust to an organization's changing needs.

I knew implementing even a portion of it wouldn't be easy. There would be pushback, a reluctance to let go of the familiar, even if it failed. But we needed a model that operated on the principle of "least privilege." Where every access request was a rigorous interrogation, each login was a fresh check-in. There are no more permanent keys, only temporary permissions for specific tasks. Not just who you are (doctor, nurse), but what you need (specific patient file) and why you need it (treatment plan).

In the months leading up to this specific event, I had been working out a plan to get our organization from where we were to where we needed to be from a security perimeter and controls standpoint. Like most industries, modern healthcare has seen the security perimeter change dramatically from a specific place to just about every place. The need to access resources and the ability to support the delivery of value and care, no matter where that happens to be, has been moving rapidly to table stakes. Bringing the perimeter down to an atomic level, where each entity needing access was isolated and

controls enforced at the level of the speci c resource needed. Nothing else was going to be critical to doing that. ZTA could make the model of that "default deny with access only granted by exception" a reality.

With that in mind, one of the only ways to get the plan I had put in place was to ensure the organizational and operational impacts were dramatically minimized. Change is hard enough for individuals and organizations, so implementing what amounted to a complete culture change (from granting access to everything and denying by exception) and technology adjustments must be treated delicately. Service accounts and vendors represented one of the most signi cant risk vectors and the entities we had the most control of and could impact immediately. So that is where we had been working, and it proved to be our saving grace in this instance.

Before implementing our ZTA strategy, service accounts were often reused for multiple services. For vendors, that sometimes meant they would get access to a service account to do one action or capability, and there was often a dramatic expansion of access scope because that speci c account got used elsewhere. We started with access via VPNs and slowly ratcheted them all down to minimum needs and documented the associated accounts and sys tems. We then spent time creating speci c service accounts for the services and locked them down to the least privileged across the board. This caused a dramatic increase in service accounts, but it also caused a signi cant decrease in associated risk.

So when I opened my laptop back up and dropped into the chat channel with the incident team, I saw they were already on it. They had identi ed and disabled the speci c suspect service account and were validating the traf c on the VPN before moving it into a disabled status. They were able to con rm that the service account was only associated with a minimal number of systems and that disabling it would have no impact other than on the speci c use cases related to Company X. The VPN had been trimmed down to only allow the minimal ports and any other traf c had been stopped at the door. I thanked the team and observed the shutdown of the VPN. Afterward, when reviewing my notes, I noticed that this speci c account and company was one of the overly permissioned ones that had seen a massive decrease in access only about a month prior. If we hadn't already been on the ZTA path, I am unsure what would have happened.

Sharpshooter Tips

- Identity is the security perimeter, which should only be opened by exception on a case-by-case basis and closed as soon as it is no longer needed.
- Start with the entities and identities you have the most access to and can control. Vendors and other third parties should be priority targets.
- Do not try to do everything at once. That is a recipe for failure when implementing ZTA. Current business processes are based on current

infrastructure and security models. Change them too quickly, and your efforts will quickly be shut down.
- ZTA will one day be the self-evident standard, but until then, it will feel like you are swimming up a waterfall and trying to explain it to folks.

Misfires

- Never reuse service accounts. One service = one service account.
- Do not over-privilege service accounts. Unfortunately, this is common because giving them more access is often much easier. After all, identifying all the interactions they might need to perform at a system level takes a lot of work.
- Do the work and figure it out. The future you will thank you.

CLOUD FIRST ADOPTION AND MIGRATION

Why are we in the data center business?

The tense silence of the Network Operations Center was like a heavy blanket had been dropped on the entire room. Panic flickered across the faces of the engineers as the primary data center status board blinked an evil red. Minutes became an eternity as they desperately tried to reach the secondary facility. Then reality started to sink in: the primary data center was hard down, and the secondary was unreachable. Both data centers, the supposed failsafe fortresses of our digital lifeblood, were down. An unknown facilities issue had turned our entire IT infrastructure into a cold, silent tomb.

As the clock continued to click, it became frighteningly clear that this wouldn't be an easy or quick fix. Amidst the chaos of recovery and business continuity that stretched from hours to days, many things came to light. People, processes, and technology were a mixed bag of good and bad. However, one thing was clear: few elements could be considered outstanding or modern in our data centers. We were a well-oiled machine, but that machine was designed for a bygone era. We weren't in the data center business; we were in the healing business.

Historically, legacy institutions are a fortress of data. Financial information, patient records, personal information, you name it – everything residing within the confines of their own data centers, a physical manifestation of control. But the world has moved on, and so have the threats. Solutions are no longer a single, monolithic instance of technology and data that can be locked away in a room. Instead, the modern world is increasingly built on composable services that require hybrid connectivity to implement, operate, and support at a speed and scale. A speed and scale that requires focused talent and resources to maintain. As a security leader, I knew clinging to

outdated practices was a recipe for disaster and could not provide the level of resilience needed going forward. The irony hung heavy in the air – why were we still in the data center business? Why waste resources replicating what cloud providers could do better, faster, and frankly, more securely?

Sharpshooter perspectives

SSP1 We all fear this moment when we don't realize our accepted risk. I don't know the whole story, but I know a few things that would have averted it! Demonstrate proactively that you have disaster recovery (DR) planning and that it works. Are you testing recovery and backup every month? What third-party relationships do you have? How are those structured? What dependencies exist? How have you accounted for those in your DR planning and preparedness to ensure you have what you need in your shared responsibility? It sounds like you shifted responsibility too much and figured you were covered with your cloud and network providers when, in fact, you were not. It was not stress-tested ahead of time for this type of disaster. It is better to plan and prepare in advance and learn from the lessons of others than to ignore, neglect to investigate, test, evaluate, apply due diligence, or make assumptions. Otherwise, you may only discover in a crisis that you're significantly at risk. Cover your A**ets.

SSP2 I want to understand how the situation happened in this story. Most upper executives have heavily pushed for cloud strategy for every company I have worked for except for the defense contractors. Usually, it does not save money, but it adds several capabilities that aid recovery and availability.

SSP3 We are still in the data center business because it is cheaper. I run a hybrid environment and use a decision tree to determine if something will be hosted within my co-location data centers or on a Platform as a Service (PaaS). It would be nice to go completely cloud, but there is a very dominant limb on the decision tree called "cost." The cloud was initially advertised as very cheap, and in some cases, it is, but many solutions would cost up to 50% more if hosted in a cloud.

Target grouping

In the past, the idea of having a corporate data center where all IT resources were located, supported, and managed was the norm (and in some critical sectors, that will probably always be the case). The costs to stand them up were enormous, though, and their operational aspects required skill sets and talent profiles that were often wildly divergent from the business they were put in place to support. Fast forward a few decades, and running your own data center, your own private "cloud" where you keep everything, is becoming far less in fashion than renting space in someone else's. Cloud computing is just renting time on someone else's resources in someone else's data center. An infrastructure that they are 100% dedicated to running and operating at peak

performance as their primary business. Organizations not focused on the specific needs of running a data center struggle to manage every aspect at a high level, especially when those resources could be better utilized elsewhere. Each year, it makes less sense to maintain control over all data center operations unless specific compliance or safety reasons, such as in the military, require 100% control. Otherwise, the effort and resources invested will likely yield less value than outsourcing, pulling you away from your organization's fundamental mission.

To stay relevant and growing, organizations need to develop a strategy to determine the most appropriate place to put resources. Unless you are in the data center business, running your own data center at a large scale is not the best place for your resources. I am not suggesting that all functions move to the cloud or that we should eliminate private data centers. We should first look at modern architectures and hybrid options and balance on-premise and off-premise resources to concentrate on core business functions. At the very least, organizations should look at co-locating facilities that handle everything that can't be a core competency. That co-location may be putting physical servers at a location purpose-built and maintained for IT systems or using a private or public instance at an established cloud service provider. Keep what needs to be on-site local, but everything else should be placed where it can be best maintained and supported.

So, what does this have to do with being a CISO? Well, protecting the data and resources of your organization needs to happen wherever it is being transacted, transmitted, or stored. That location is probably better someplace other than your walled garden of slowly decaying infrastructure. The cloud isn't some temporary space. It can be a secure, scalable network constantly updated by security professionals and not overworked IT staff. The organization wouldn't be managing physical machines but configurations, processes, and a modern infrastructure described by code, not legacy metal. Identity, not a physical perimeter, would be our security model. Zero Trust, a concept where constant verification trumps blind trust, would be our watchword.

It took a lot of time to get everything back up and operational. We scrambled and enacted our DR plan, but the truth was that our on-premise data center was a creaking monolith, held together by duct tape and overworked engineers. The cost to recover was staggering. Many systems didn't come back up, and restoring operations to total capacity was more about replacing and updating infrastructure components at the data center than ensuring databases and solutions were working.

In the aftermath, the board demanded answers. They were tired of the constant disruptions and the ever-escalating IT budget. There were many contributing factors, but the actual cause of the failure was a physical component at the facility that had deferred maintenance. Something that would most likely not happen at an organization whose primary business was owning and operating data centers.

This event was enough to cause a shift in the organization—to a cloud- rst approach. Our on-premise network, once a physical barrier, became a bridge to the cloud. We embraced Software De ned Networking (SDN and PaaS solutions, creating a hybrid architecture. Our physical data center remained, but it was moved to a co-location facility that specialized in that work and it started to look like just one node in a larger, interconnected landscape. The logical network, encompassing cloud and on-premise, became our new frontier.

Cloud adoption wasn't without its pitfalls. Agility, a signi cant selling point, could be a double-edged sword. Spinning new cloud instances was fast but could also lead to security shortcuts and budgetary impacts. We had to balance leveraging the cloud's speed while adhering to strict security proto cols. Security became much less an afterthought and much more the founda tion upon which our cloud journey was built. But that is a story for another time.

Sharpshooter Tips

- You can do everything right from a technology and controls standpoint but still struggle with business continuity if things outside your control fail.
- Stay modern in your approach to the organization's security and infra structure, which you rely on to operate your role's capabilities and functions.
- Sometimes, it takes a major event to move people from the old way of doing things to a better way. Have an idea of what that new way looks like so you're ready to guide the conversation when the opportunity presents itself.
- Monolithic architectures should be avoided unless required. Modern architectures are composable solutions and are often much more resil ient and agile.

Misfires

- Stick to your strengths and specialties. This counts at an organizational level as well.
  - Don't pretend to be an expert in something if you can't be that expert and your business relies on that expertise.
- Don't underestimate the physical risks to your technical world.
- Small things can have signi cant impacts, and deferring the "non-prior ity" items for too long can create high-priority problems.

It isn't work from home. It's work from anywhere

The of ce was just about empty, with the only noticeable sounds coming from the HVAC systems circulating air at a constant and comfortable temperature

like a white noise metronome. A single employee sat at his desk while I typed away in my office. Emails and virtual meetings were the flavor of the day as I filled the hours of this otherwise average weekday. The previous week, I sent all the employees home to work remotely for a disaster recovery and distributed work experiment. It wasn't a response to any mandate or an effort to recruit and retain talent. It tested whether the team could operate at expected levels while geographically distributed and remote in the case of a natural disaster that prevented them from coming into the office. The employee in the office with me had asked for an exception to go to the office because he felt too distracted at home and couldn't accomplish the tasks that he needed to do. I felt a need to be still on-site and "lead from the front," leaving the two of us as the only residents of the entire floor while the business continuity exercise played out.

Things had started a bit awkward, with the first week being just this side of chaos, but by day 7 of the 14-day experiment, an interesting trend began to appear. Operational effectiveness increased while ad hoc conversations and collaboration took a nosedive. People started to communicate at all hours of the day, and "work hours" blurred into a blend of all days and differing circadian rhythms. Still, work satisfaction metrics jumped higher than I had seen in over 20 years as an executive leader.

Little did I know that less than 12 months later, the entire country would be locked down and scrambling to figure out how to keep business flowing while being anywhere but the office.

Sharpshooter perspectives

SSP1: You'd make a great captain who goes down with his ship. Did you go down with your network during Covid, or did your network survive thanks to some proactive preparation? As I read the story, it's clear that the CISO is leading by example and fostering a community of loyalty with practical outcomes. Staff often become "busy" and accomplish nothing that moves the needle in the workplace, directly reflecting poor leadership. If you have busy people who aren't effective, look at yourself and your culture and figure out where you can impact it to move the needle. Excellent work ethics, commitment, and loyalty start with trust and relationships. What are you doing as a leader to connect with your people, professionally and personally, and take one for the team and be that leader in the office, anchoring the team so others can be home with family on holiday? Lead by example, foster mutual love and respect, and see team spirit, commitment, and retention rise in the workplace.

When an organization takes the time to perform disaster preparedness, run/playbook incident response, and impact studies with the right stakeholders for the right threats, the most important outcome is what the organization does after the exercise. The exercise raises awareness and collaboration but doesn't address process improvement, implementation of new tactics,

improvements in policy and procedure, or proactive hardening and preparation for a disaster. Due to politics and a lack of leadership, many organizations "get busy" and do little to nothing following such exercises, failing to lead and proactively reduce risk. Great leaders are great planners! Immediately following exercises, set expectations for an after-action report, recommended actions to be reviewed by key decision makers, and a road map for short- and long-term goals to improve operations to reduce risk. "If you fail to plan, you are planning to fail." – Benjamin Franklin.

SSP2: What a great leader to test the ability to continue operations with a distributed workforce. The great social experiment in 2020 showed that many people can be highly effective while working remotely, and some cannot. I applaud the professionalism of the worker who self-identified that working from home was not a good option for them. When it comes to IT workers, management expects that they can work from anywhere. Let a critical system go down, and you'll see people working extremely hard from home to get the system back up! So if they have to work from anywhere, why can't they work from anywhere? I am amused by the old-school CEOs who require everyone to return to the office since "we cannot be productive when remote," and they don't recognize that everyone is remote when you have people working together but distributed in offices around the globe. They have work processes and practices that work for multiple offices, so why can't it work with practically everywhere being an office? These same CEOs said, "It will never work." IT leaders showed that it could work. The narcissistic tendencies of CEOs needing to think they are in control drive these decisions and not meaningful data. They love to quote the studies that support their position, even when they aren't relevant while ignoring numerous studies. Quite frankly, I have been a remote worker since leaving a high-security job almost 20 years ago, where everyone had to be on-site working shoulder to shoulder due to the security requirements.

SSP3: I have had to fight for people's ability to work remotely several times, long before Covid. I am ecstatic that you did this as a business continuity exercise. Senior management frequently asked me, "How do you know what they are doing?" In the job description, I would explain that I measure my work by product and duties. From some execs, this statement perplexed them even more. If I have someone whose duty is to review vendors' security, I will notice that the reviews are not getting done. I also review work products (vendor reviews) with the employee. This usually leads to another question: "How do you know if they are busy enough?" The answer is a couple of ways: (1) I usually do most of the duties each employee has at some time and have an idea of how much work each entails; (2) I ask the employee how things are going. In addition, I usually have a set of metrics that I am monitoring. The thing about most security professionals is that they are curious and are typically concerned about a broad number of risks. Most of the time, I don't have issues getting them to work; the real issue is getting them to work less because burnout is a real issue in the profession!

Target grouping

If the pandemic taught us anything about work, the traditional ideology that all roles required you to be at some centralized location to produce valuable work products was untrue. In many cases, the ability to effectively execute a function must be enabled from anywhere (geo-location independent) to gener ate value. It is one of the core concepts behind ZTA, where the location of the entity doing the work doesn't matter. Still, the identity of the entity and the ability to enable the work to be done regardless of the geo-location is what matters.

Information security is one of those disciplines that falls squarely into the realm of functions that do not require a speci c geo-location for the work to happen. The ability to acquire and utilize resources dramatically increases when you remove the requirement for constant geo-locked talent. Yes, it is still better for collaboration and knowledge transfer for people to be in the same physical space, but it is not something that needs to happen all of the time. Suppose the focus is on enabling the work to occur regardless of where or when it is done. In that case, the resources tasked with doing it can be force multiplied and aligned to increase effectiveness and worker satisfaction. Then, when you do need to have your team work in a geo-speci c location (for team building, collaboration, and alignment items, as an example), the same level of capability can be accessed and enhanced to create a culture that focuses on the result, instead of the legacy mechanisms on how to achieve it.

When the information security function is structured this way, enabling other business areas to do the same is much easier. To do this in cyber-se curity, you need secure, compliant, and privacy-enabled systems and pro-cesses in place. However, when those are ready, the Security by Design principles and models can be adapted to other areas where this could be an option. It is a "win–win" situation for the larger organization and the employee.

The nature of business and work is different from what it used to be. The ubiquitous nature of connectivity and the inherent composability of modern solutions that take advantage of that have established a new norm for both business and cybersecurity needs. Any CISO who hopes to have long-term success needs to embrace this and structure their programs around it, or risk becoming ineffective and ultimately irrelevant to the needs of modern organi-zations and work environments.

Cybersecurity needs are everywhere, all at once and all the time. Shouldn't your program be structured to address those needs from both the systems and the workforce?

Sharpshooter Tip

- Legacy models and concepts must be reviewed and reevaluated regu larly. Work location is one critical area. Enabling the workforce to "work" from anywhere allows the ability to recruit and retain talent

from a larger resource pool. It also builds a higher level of resiliency and adaptability for the inevitable emergencies that could make a location-dependent function unavailable.

Misfire

- Not everything legacy is terrible, and not everything new is good. One of the unintended consequences of geo-diverse working is a decrease in team connectedness. Having a plan or model in place to address the personal dissociation that can happen is critical to the long-term success of your program and team cohesion.

Iteration is innovation

"Where is the 'Wow' in the Board deck? I'm having trouble nding it." I stood there, a little stunned by the question. We had taken several weeks to work on a concise, understandable, and informative set of slides for the annual plan ning meeting with the Board of Directors. The cybersecurity program status was clear, and the projected goals for the next 12 months illustrated a rational and risk-reducing plan that would increase organizational compliance with out any signi cant increases in budget or staff needs, but for some reason, all that was being overlooked by the senior executive who I reported to at the time. Knowing I'd probably be sorry for asking, I decided to go for it and say, "What do you mean by 'Wow'? Looking at this, I see quite a bit to be excited about." A raised eyebrow and a more stern than it should have been voice replied, "When we hired you, we were looking for someone who could help kick our program into high gear. I don't see anything groundbreaking here that would lead me to believe that. What secret sauce will we show and sell to the Board to get them to increase support this year? What solutions must we implement to stay ahead of the bad guys and the competition?" I knew where this was going, so I took a moment to gather my wits about me, then said, "The secret isn't in the ingredients. Like any good chef, the innovation is in how you use the ingredients you have to work with." Intrigued but still skeptical, he said, "Alright. Show me."

Sharpshooter perspectives (SSPs)

SSP1: All too often, leaders are myopic, focused on a speci c short-term met ric, goal, or achievement instead of a long-term transformative process. CISOs win the cyberwar one battle at a time, with a war plan in place, always keep ing perspective and the battle eld in mind. Great CISOs have a comprehensive situation report (SITREP) integrated into their operations, KPIs, and metrics. They structure project management into bite-size tasks that ensure success and enable the team to operate at the speed of business with clear priorities. Achieving this at scale in a high-paced, complex technical environment is

much harder than one might think, yet it is a challenge every CISO must now embrace! A risk-based approach is the core foundation for all prioritization, ensuring the best outcomes in long-term success. For example, current conditions in patch management exist where bad actors, on average, have exploited new patches within 14 days while companies strive to obtain "N" state patching over a 30-day day. You are at risk with every applicable patch, and your highest-value assets hang in the wind 50% of the time. What are you doing that is risk-based to ensure your most important assets open to exploitation are patched first, in days or weeks instead of months? Embrace the principles and practicality of continual learning and improvement towards the essentials of risk management to proactively reduce risk and recover quickly when you have an incident.

SSP2: This makes me think about how I approach potential security products. Here is my thought process.

1. Does it address a significant risk in my risk register?
2. Did I miss a significant risk if it isn't on my risk register?
3. Does a solution I own but haven't implemented solve the same issue?
4. If this vendor will solve one of my significant risks, is this the right vendor? Are they hoping to make a big splash and get acquired by one of the big security dogs? Does my contract protect me during a buy-out?
5. If I buy the solution, do I have the staff required to implement, maintain, and use it, or will it become an expensive boat anchor?

By considering the implications of these questions, one can sort through the vendor hype and help avoid a potentially costly purchase and diversion of time to nonproductive activities.

SSP3: My most significant "Wow" moment was when one of my security engineers installed our first FireEye appliance in 2011. We had a bet on how many infected devices we estimated we had in the environment. He bet 10. I bet close to 100. We were both wrong, and I bought the engineer lunch for being the closest. The first day the application was plugged in, there were no alerts. On the second day, there were no alerts. Finally, on the third day, one of our employees hit a drive-by-download, infecting their machine. We were lucky to have no infected devices because absorbing the new technology took nearly a year. Based on the intelligence from the FireEye devices, we restructured our patching to patch frequently attacked software. We restructured our URL filtering firewalls to catch more. We also reworked our incident response program. Overall, one "Wow" technology took us at least 2 years to integrate fully. The biggest lesson from all of this was that our current patching program caught a lot of attacks, which appeared to be why we had next to no infected devices in the network. There is no "Wow" in patching, but it proved to be the most critical control in our arsenal.

Target grouping

While “showing them” the “Wow,” I covered four primary points to drive this home:

1. A Secure Future is Fueled Through Daily Iteration

   As CISOs, the allure of rapid innovation through sudden technological advances constantly tugs at our attention. The industry’s breakneck pace seeds the illusion that security strategies must match that volatility by reinventing continually. However, the most enduring innovations strengthening enterprise cybersecurity take shape through systematically iterating existing approaches, not chasing sparks that flash and disappear.

   Look at multifactor authentication (MFA), for example. Now a security staple, it arose from decades of incremental enhancements to access controls – password complexity policies giving way to one-time pins before the eventual effectiveness of biometric factors compounded MFA into the gold standard it now represents.

   The roots of any seismic shift generally trace back to iterative progression built up behind the scenes until a tipping point into mass adoption triggers. In cybersecurity, this means recognizing and doubling down on the power of recurring marginal gains made over long timeframes.
2. Compounding Gains are Achieved by Tuning Out the Hype

   Over my tenure as a CISO, the single most dangerous distraction gnawing at essential progress has been hype over the latest bleeding-edge security solutions. It’s easy to get swept up in the constant barrage of vendors pledging revolutionary protection powered by AI or quantum-safe algorithms.

   However, authentic innovation in security arises more from pressure testing existing controls and processes rather than rip-and-replace implementations built on promises that are not proof. Actual transformation compounds not from one-off deployments when threats emerge but daily stress testing of the fundamentals currently in place.

   Staying focused on those less glamorous but crucial iterative security layers bears real fruit if it persists steadily over the years. Sort of like the “corn ake effect” of Yankee Stadium being built by transporting and placing small loads of debris day after day until the massive stadium took shape through sheer cumulative effort.

   Similarly, something as basic as mandatory password changes done quarterly since the early 2000s led to significantly more hardened authentication landscapes now made possible by stronger, secondary controls branching from that initial seed.
3. Directing Iteration Through a Risk-Based Lens

   Managing security through an iterative rather than reactive lens requires constantly filtering efforts through a risk matrix focused on

likelihood plus impact. This method allows for accurate targeting of controls and processes that need priority attention because risk reduction potential is highest there.

For example, recurring penetration testing around high-value data assets prioritizes one-off pen tests on less sensitive systems. The volume and velocity of testing on crucial areas reveal more vulnerabilities over multiyear spans, allowing much more signi cant risk reduction through iterative remediation.

That risk-based approach also includes consistently reevaluating assumptions on existing controls as part of critical iterative cycles. Regularly question the status quo on current processes with the same zeal as vetting new technologies.

Tuning out hype always starts by cultivating a learning mindset on previous decisions, not a rigid belief that those choices remain permanently sound.

4. Confronting Complexity through Consistent Steps

CISOs need to pay special attention to recognizing innovation, not in implementing silver bullet offerings but in doubling down on amplifying risk reduction through recurring, incremental improvements, particularly focused on known critical assets.

Embarking on massive digital or cloud transitions may seem mandatory to rapidly advance defenses, but teams left bruised by unsuccessful big bangs often regret skipping the less ashy block-and-tackling required to shore up controls on legacy layers before trying to re-architect them.

True innovation arises from a fusion of knowing precisely which small iterative actions today manifest into maximum impact down the road while accepting that the exact shape of what emerges may shift as progress unfolds. But staying doggedly devoted to those marginal gains tees up seismic change in time, even if initially con ned to existing technical debt.

After all, iteration is born from intent and resilience, and the engine generates lasting innovation. And that's what will continuously harden the next generation of cybersecurity. Unfortunately, after all that, my boss at the time was more interested in the ash of the solution than the core of it and decided to purchase a "cutting-edge solution to accelerate the environment to the next level rapidly." Not sure if they needed to spend the budget or if something else was at play, but 2x the money went towards adopting a new solution that turned out to be a massive failure and ended with the executive " nding a new opportunity." You can't win them all, I guess.

Sharpshooter Tip

- You can do everything "right" and still not get the desired result you are hoping for.

Misfire

- The more you know the hidden and nonobvious motivations of the stakeholders involved in your program, the better off you will be. By not recognizing that the criteria for success were signi cantly different, achieving the hoped-for success in this instance was hard. Do the pre work even if you think it isn't needed.

Agile development shortsightedness

As a newer leadership member of the team, I focused on listening and learning in the rst 30–60 days while building trust. I was especially focused on the data in the SIEM, as I needed to process the information in both structured and unstructured manners to achieve consistent, automated, simple queries such as IP and WHOIS lookups, reputational queries, correlations, enrichment queries, and malware attributions with reasonable levels of trust.

I observed a wide diversity of tools and tactics in SOC operations and a need for more consistency and understanding amongst all staff, seeking to standardize the core foundation of SIEM processing to help the SOC focus on analysis instead of click-fatigue lookups and queries. The leaders of SOC operations were "chief doers" who earned their role by working harder than the others, not necessarily individuals with people skills or leadership cultivation and mentoring.

The Agile Development Team, who had largely been with the company for over 10 years, were still young, worked odd evening hours, and often from home. They informed me that we had state-of-the-art arti cial intelligence within our tech stack. Documents of all kinds were dropped into an unstructured database. They could easily be searched and retrieved without any effort, quickly and on a massive scale, according to the Agile team. Agile team members were motivated with monthly management by objective (MBO) metrics for bonuses, focused only upon short-term requirements.

Sharpshooter perspectives

SSP1 Listening and building understanding is a great strategy when establishing yourself in any new security leadership role. Since a rehose awaits one in any new security role, nding the right balance between listening and taking action is a dif cult judgment call that is enhanced with experience.

Playbooks with de ned process ows are essential in any SOC operation. Create the list of playbooks needed and focus on developing and implementing the most critical rst. In critical incident situations, a database of documents that can be searched and enhanced with AI capability will never replace the ability of a seasoned professional who can instantaneously decipher a problem and initiate the proper containment.

Knowing the author is a seasoned incident response and remediation professional, I predict that after assessing the tools and ensuring they are adequate

and that playbooks are in place, the focus will be training and skill development for the SOC staff, followed by team building.

SSP2 Cultivate a culture of "automation first" in the SOC team "doers" so that they can be trained to manage, mentor, and train staff rather than spend time clicking through incidents. Based on the use cases provided by the SOC team, the Agile Development Team should be able to automate specific process flows in the SOC. If the team has issues developing this, they may not have the right technology or skills.

SSP3 Huge maturity red flags here. Competent people engaged in heroics (ad hoc) is what this sounds like to me, combined with a total mismatch of incentives to actual work needed to address the issues. The culture issue is one of the first things that jumps out at me. In immature programs, it is not uncommon for the most technical to get the lead role and be escalated into management. It is also one of the biggest reasons these managers struggle with their roles. Management and technical expertise are wholly different, and different talent profiles are needed to succeed. This is one of those situations where everyone needs to come to the table and have some hard conversations. What works in a "Main Street" organization does not scale to a "Wall Street" level without significant standardization, role clarity, and leaving the urge to be everything to everyone behind. When organizations grow too fast without considering factoring solutions into repeatable patterns, they are bound for issues and avoidable chaos.

Target grouping

In hindsight, I was hired to acquire a company to buy versus build, and the purchase fell through. My role was never to fix and develop the solution in-house. I was left with broken pottery, and management wasn't all-in on helping me fix the problem. Not one to fail, I quickly recognized the actual root causes, making it impossible to succeed: cultural challenges, lack of leadership, and transformative gaps.

You will fail without a vision, actionable plans, and a proper foundation. A roadmap was created for the prioritized data ingestion, parsed management, storage requirements, and how information can be processed intelligently for the intelligence and MSSP operations lifecycle. Once this plan was in place with all considerations, we bit off what we knew we could, slowly untying the Gordian knot that was in place in operations that was created over 10 years prior.

We started with 93% of data being blobbed, executives being snowballed, and smoke and mirrors from the DevOps team. After a 3-year transformative journey, we ended with 100% of all data being parsed, then enriched and correlated in an SOAR, then automated through multiple tools and lookups formerly performed by staff, saving thousands of dollars in monthly productivity and consistency in ops. We also ended with truth and transparency instead of what we started with, a true transformation, reflecting a cultural change

where we learned to accept our current state and work towards maturity, celebrating our current state and maturity gains instead of trying to make everything look good despite the current state – no matter what that state is.

Automation was one of the most challenging processes due to the complexities one learns when attempting to automate. You might think you can easily automate things until you try, and then you realize the process is not documented, and there are twists and turns you didn't expect – resulting in a mess. In short, automation is challenging to turn out consistently!

Start small with automation, streamline processes, tooling, people, and technology. Audit it heavily until you have the expected results, then scale up. This is critical as you scale projects with additional tooling over an extended period. Embrace the crawl-walk-run concept so you don't get overwhelmed with all the problems that automation can reap, focusing on the more accessible automation elements within your project first. In this case, what started with simple query lookups for IP and domain, followed by more complex malware attribution and correlation queries.

Another key challenge was the wrong motivations for the DevOps team, where MBO was used to evaluate and provide bonuses for staff. This incentivized staff for short-term goals, nothing long-term. They also had a short-term mindset since the development industry was moving towards agile computing with short sprints and away from the long-term planning approach of SDLC. This shift resulted in a generation of programmers that grew up in a culture where they are rewarded for the here and now, nothing long-term, and not many experiences beyond quick sprints. This mindset had to change to include long-term strategic goals and motivations built into how they received financial rewards, bonuses, and growth opportunities. It's not hard, but it is essential, as leaders, to ensure we motivate staff in the right way to incentivize the proper outcomes.

Any time a tech team advertises shiny new capabilities and can't demonstrate actual results in production that is a major red flag! Always trust but verify. Discuss different frameworks, challenges, and approaches with various subject matter experts across the industry.

Sharpshooter Tip

- Know your people, what motivates them, and how things operate on the floor. Research solutions from all directions – bottoms-up, tops-down, as a team, and unify towards a consistent outcome. This all takes time, but investing in your people with a focus on trust results in positive change, especially when starting in a toxic culture.

Misfire

- If anyone tells you the latest shiny tool will solve all your problems or do "all these amazing things," your internal red flags should go up. Find trusted colleagues to verify, do your homework, and approach cautiously.

Data loss watching

I was a CISO at a technology company that held government contracts. After assessing the technology environment, I found that we did not have data loss prevention (DLP) or data classi cation in place. I worked on a roadmap and budget for both projects and presented the strategy and implementation plan to executive management.

One VP was very supportive and stated, “At least two new technology companies have been founded using our intellectual property (IP), which was taken from our company.” Unfortunately, I received pushback from the VP of Engineering, who was concerned about the program slowing down his projects.

Considering the VP of Engineering’s concerns, the team worked to put the tool into detection mode for an extended time. This allowed IT to test whether the endpoint agent interfered with other software in the environment. In addition, it allowed the newly established DLP team to get a baseline. Implementation began with a small number of individuals within the Information Security Team and spread to the entire department.

As part of the rollout, I communicated with the department, describing the tool and how it worked. Because the tool was in detection mode, the alerts could be better described as “data loss watching,” but by the time we investigated an alert, the data had already moved. We could start to see how information moves within the environment. After 6 months of testing, the head of the DLP unit pulled me aside to discuss a concerning alert. Yesterday, one of the senior engineers moved a terabyte of les onto a personal USB drive.

Sharpshooter perspectives

SSP1 What intellectual property (IP policies are in place? I assume there are policies in place that prohibit taking company documents. If the investigation determines the download contains company les, legal rami cations for the individual may occur. However, without an investigation, I would not presume that the les are company-related. I’ve seen company-owned computers with enough video les to rival Net ix, so this could be something other than IP theft.

SSP2 “The lady doth protest too much, methinks,” as Hamlet might say about the VP of Engineering. Sometimes, people know they are doing something they shouldn’t but still do it because they feel a sense of entitlement that speci c rules don’t apply to them. Developers and intellectual work product teams seem to use this pattern more frequently. When someone spends a lot of their intellectual capital in creating something, a sense of personal ownership remains even when it is obviously the IP of the organization that paid them to do it. I am not saying this is the case here, as I have seen some less malicious things cause similar alerts. However, if it looks like a duck, quacks like a duck, and swims like a duck, it is reasonable to assume it is a duck.

Target grouping

The DLP unit had detected an engineer loading a terabyte of files onto a USB drive. It was discovered that the senior engineer had received a position at a competitor but had not disclosed that they were leaving. The information they had moved to the USB was company-proprietary, and the investigation took several weeks to determine the extent of the files they had taken. They were fired from their current position, and legal action was threatened unless they returned the files.

Sharpshooter Tips

- Implementing DLP software shifts the cultural shift to protect the company first. Many executives hold an optimistic belief that most employees are ethical and will not take company property.
- During implementation, be prepared for your team to find individuals stealing company information. Work with HR on the disciplinary process. Because much of the theft occurs when employees leave, coordinate with the Legal Team as they may pursue legal action against the former employee.

Misfire

- Many DLP implementation plans underestimate the resources needed to review and follow up on alerts. In this case, an internal team and the MSSP handled the workload, avoiding a misfire.

Index

A

Agility, 170
Alert fatigue, 115, 116
API, 133
Authority to Operate (ATO), 24 , 128
Automation 75 , 117, 128, 135, 153
Automation rst culture, 179
Awareness programs, 44, 45, 120, 121, 124
Azure, 76

B

BAA, see Business Associate Agreement
BCDR, see Business continuity and disaster recovery
BCP, see Business continuity plan
BIA, see Business impact analysis
Bitlocker, 25
Blacklisting, 133
Bugbear, 89
Business Associate Agreement (BAA), 76
Business continuity and disaster recovery (BCDR), 78, 79
Business continuity plan (BCP), 29, 146
Business impact analysis (BIA), 62, 137, 139, 143, 147
Business risks, 11, 27, 65, 66, 119

C

California Privacy Rights Act (CPRA), 12, 74
Capability Maturity Model Integration (CMMI), 82 , 84, 96–98
CAPTCHA, 132–134
Center for Information Security (CIS), 14
Certi cations, 8–10 , 93
Certi ed Information Security Manager (CISM), 8
Certi ed Information Systems Security Professional (CISSP), 8, 9
Challenges, operational, 67, 68, 83
Chief Doers, 68, 69
Chief Information Of cer (CIO), 22 , 109, 113, 115
  adopting a C.R.A.S.H. mindset, 30
  breaking through denial, 42
  budget challenges, 23
  handling power plays in executive engagements, 70
Chief Technology Of cer (CTO), 4 , 19, 20
CIO, see Chief Information Of cer
C&IS, see Computer and Information Security
CISA, see Cybersecurity and Infrastructure Security Agency
CISM, see Certi ed Information Security Manager
CISO, sic passim
CISSP, see Certi ed Information
 CISO, sic passim
 CISSP, see Certi ed Information
  CISO, sic passim
  CISSP, see Certi ed Information
   CISO, sic passim
   CISSP, see Certi ed Information
    CISO, sic passim
    CISSP, see Certi ed Information
     CISO, sic passim
     CISSP, see Certi ed Information
      CISO, sic passim
      CISSP, see Certi ed Information
       CISO, sic passim
       CISSP, see Certi ed Information
        CISO, sic passim
        CISSP, see Certi ed Information
         CISO, sic passim
         CISSP, see Certi ed Information
          CISO, sic passim
          CISSP, see Certi ed Information
           CISO, sic passim
           CISSP, see Certi ed Information