CHAPTER 1

If I Had a Time Machine

> The real trick in life is to turn hindsight into foresight that reveals insight.
>
> —Robin Sharma

Imagine going back in time to watch and listen and change things. Where would you go? And to what point in time?

Do you have the knowledge, tools, and influence to change things for the better? If so, who would you interact with to alter the specific outcome(s)? What one (or perhaps two or three) things would you do differently, and why?

Yes, you can ponder these questions about virtually any area of life. However, this book specifically addresses cybersecurity incidents or other emergency situations that contain significant cyber components that have in the past, or are in the present, or will in the future, impact global organizations in substantial ways.

Stretching further, society is growing even more reliant on resilient infrastructures that demand functioning cyber protections that involve people, process, and technology components. If we fail, the consequences will be dramatic in real life.

This journey must start with the lessons from the past. We can learn from stories from global cyber leaders and practitioners who have been through cyberattacks and come out stronger. Along the way, we will

point to frameworks, checklists, standards, protocols, white papers, and other helpful materials.

If we are going to be equipped for the inevitable cyber storms that are coming in the decades ahead, we must learn from each other and improve faster than the bad actors who are causing such online destruction. In doing so, we first explore what works and is repeatable regarding cyber incident response.

STARTING WITH THE UNKNOWNS – OR NOT?

"I don't want to know, and I don't care to know. If I don't know about it, it does not exist." Shocking, but in fact, there are many business leaders who think this way.

The truth is that sometimes, some data takes only a minimal effort to discover, and when you realize the type of information that is available out there and accessible to anyone (including malicious actors), then you will have no choice but to care. As the chief growth officer at Privasec (*a Sekuro company*), a top-tier and agnostic cybersecurity firm, Shamane leads the security outreach strategy team, spearheading industry awareness initiatives while working closely with the CISOs (chief information security officers) in bridging their business gaps. She met Todd Carroll, a former 20-year FBI cyber intelligence leader, virtually, in a cyber security summit she organized, where he shared an intriguing story. Todd walked through one of the real-world findings that CybelAngel's data leak detection technology came across a few years ago.[1] CybelAngel detects exposed data, devices, and services outside the enterprise's perimeter, enabling remediation before the exposure is weaponized. In this instance, it detected several pieces of information that exposed a bigger issue involving several airports, their ecosystem, and exposure of their data.

The thing is, data is always being shared. The aviation industry, like other industries, works with third parties. The moment any

organization shares information with a third party, it loses visibility or control over what is done with the data, despite their best efforts or intentions.

In this case, when CybelAngel performed a search and monitoring on keywords related to airport security, they detected nearly 10,000 servers that were publicly available, on which over 400 blueprints of airports worldwide were identified, sitting on unprotected third-party connected devices, or in misconfigured cloud storage.

Some of these blueprints were extremely detailed, including the location and angle of the security cameras, revealing which were motion activated or had facial recognition capabilities and even precise information on how to access and take control of them. In addition, these blueprints contained the location of the detention rooms that are hidden from the public, runways, and the position of the fuel lines from the tanks leading to the runway where fuel is pumped into the wings of the aircraft.

There were blank signed templates of security application access forms that, if compromised, would have allowed access into the airport facilities. There were also completed security badge application forms with official stamps and signatures, and over 300 files describing safety procedures and policies. Those procedures included instructions on how to bypass the whole security system, and how to deactivate it.

There were also identity details of air marshals and departure and arrival dates, as well as the list of weapons they are allowed to carry on planes. Such intricate information can easily serve as a blueprint for a terrorist attack.

The frightening part of all of this is that the data was found on third-party servers in many countries, including the United States, France, the UK, India, Spain, and others.

It was fortunate that the findings were reported to the impacted organizations in time and the FBI and Interpol worked on closing the thousands of open servers around the globe. Imagine the terrorism

disaster that could have occurred had this information not been discovered due to a lack of interest and blind obliviousness.

As the world continues establishing even more interconnectivity, it becomes more critical than ever to position industry leaders to have better foresight before a crisis even happens.

AN ISOLATED PERSPECTIVE HAS MANY LIMITS

John Yates, QPM, is a former assistant commissioner in the London Metropolitan Police Service. He retired in November 2011 after a 30-year career. In his last role, John was the UK lead for counterterrorism and the most senior advisor to the prime minister and home secretary on law enforcement issues relating to terrorism. In this role he was also responsible for protecting the royal family and senior government ministers as well as the Houses of Parliament and Heathrow Airport.

John is currently the director of security for Scentre Group, which owns and operates Westfield Shopping Centres in Australia and New Zealand. He shared his lessons for the cyber industry from his counterterrorism days:

"One of the key roles of leaders is to keep out of the weeds and be constantly looking up, thinking broadly and identifying trends. I want to talk about a relatively little known case in London in 2010. It was a case that should have been examined in much more detail because it was one of the principal precursors to a deadly and murderous shift – the radicalization of predominantly young people – that plagued the efforts of those seeking to counter terrorism for many years and, indeed, continues to do so."

In a time where radicalization was little understood, particularly by young vulnerable people, Roshonara Choudhry, a final-year student at King's College, London, and from a good Bangladeshi family, brought two knives to Beckton Globe Library, where MP Stephen Timms was conducting his constituency clinic. Choudhry stabbed Timms twice in his abdomen.

"She missed his life organs by two millimeters. He nearly died." John further explained that Timms was the most popular MP in the country at that time, and he represented a community with a large population of Muslim residents. Yet Choudhry targeted him because he voted for the Iraq war. Despite Timms's work in the community, Choudhry had been radicalized online.

John continued, "This case was initially dealt with by the local homicide squad. It took us over 24 hours to realize that this was in fact a terrorist attack, being that it clearly fit the long accepted definition – the unlawful use of violence and intimidation for political or ideological aims.

"It was actually the first successful terrorist attack in London since the July bombings in 2005. So at the time, the case was taken over by the counterterrorism command and Choudhry was convicted and sentenced to life imprisonment.

"But we stopped there. For two years, we didn't really do anything, and then suddenly the whole problem of people being radicalized began to play out in developed countries, particularly in the Western world. ISIS emerged and the online community became an effective vector to radicalize people.

"What happened in 2010 was a significant event. What we failed to do was to identify the broader implications – that Al Qaeda and, later, ISIS were using social media and other online means to target vulnerable people – and pose the question, could this happen again and what should we be doing about it now?

"One of the duties of leaders is to take any extraordinary or unusual events and reflect on the underlying issues, to consider what the themes are that need to be addressed. Is there something that we need to be doing here in the education environment? Is there something that we should consider about the public warnings?

"We didn't do any of that for a number of years and then we got way behind in terms of our ability to understand the motivations of these people and to understand the impact it was having, particularly on young people.

"And then you fast-forward seven years, you've got a 14-year-old child in the Northwest of England being convicted of terrorism for trying to radicalize young people in Australia to carry out an attack in Melbourne on Mother's Day.

"All those factors were there in 2010; Choudhry was the first manifestation, and with serious consequences, in the developed world. We didn't open our eyes to the broader issues back then. We just dealt with it as a very serious attempted murder, and put it back in the box. We did not sit back, reflect, debrief, and consider the implications more broadly. It's something we should have done at that time, and it was most regrettable that we did not."

John's lessons are even more applicable in today's modern digital world. There is merit in studying the past and present incidents, considering the context of each, trying to gain a macro perspective and thinking about the bigger picture of what it could evolve into in the future.

When an event is looked at in isolation, it will always project a narrow view, which limits one's ability in preempting and preparing for the best defense response.

Likewise, in examining a cyberattack, it cannot be viewed in isolation. Effort and care should be taken in studying the source – is it just a random phishing attack, where is this coming from, are there other breaches instigated by an insider threat, is it a competitor that is trying to undermine your shareholder value, or did you happen to fall prey as a pawn in the grand scheme of geopolitical affairs?

When we look at the advancement and sophistication of these cyberattacks over recent years, we need to retain a holistic view of what these changing implications might mean for the overall organizational and individual risk.

Military leaders point out that capabilities take a long time to develop, but intentions can change overnight. In other words, the cyberattack impacts and response will not only center on current technology solutions, but also on what scenarios could happen in the future.

LEARNING FROM OUR PAST TO LEAD OUR FUTURE

While there are numerous management actions competing for attention, one clear priority that cuts across the public and private sectors is ensuring the leadership skills and capabilities of your team –especially the CISO or equivalent leadership role. To achieve any measure of success at dealing with cyber incidents, a CISO with the required background, accountability, training, real-life experiences, relationships, and tools to do the job is a must.

One such CISO is Mark Weatherford, currently the chief strategy officer at the National Cybersecurity Center and CISO at AlertEnterprise. Mark served previously as the deputy undersecretary for cybersecurity in the U.S. Department of Homeland Security (DHS) and vice president and CSO for the North American Electric Reliability Corporation (NERC), in addition to other senior leadership roles in cybersecurity.

While Mark was the CISO for the State of California in the mid-2000s, he experienced what organizations should *not* be doing when hiring for this vital role.

Because Mark was the first CISO in the state, it was important to him to put a face to the name of cabinet secretaries and agency heads. As such, he made the rounds to visit each of them and also to tell them about the governor's vision of Mark's statewide role and what he hoped to accomplish across state government. Mark also offered his assistance in everything from procurement to policy development to technology infrastructure to staffing. His proactive outreach seemed to be well-received and generally met with enthusiastic support.

At the same time, Mark also met the security leaders and their teams at all of the agencies. During the mid-2000s, almost none had a formally appointed CISO, but most had someone they could point to and call their security leader.

One exception was a large agency with significant citizen privacy responsibilities. Chief privacy officers were even more rare than CISOs

at the time, so privacy issues were typically part of the CISO's portfolio of responsibilities. When Mark met with the leadership of this particular agency, he encouraged them to fill the CISO/security leader role as soon as possible since they were accepting a significant amount of risk by failing to have a single point of contact to guide the security and privacy efforts of the agency.

Mark recounts what happened next:

"A few months after the conversation with this agency head, I received a call from someone who said they had just taken the CISO role at this agency and would be very interested in meeting with me to understand how they could quickly integrate into the statewide security leadership group. I remember thinking how odd it was that, even though I had no real authority within this agency and they were under no formal obligation to ask my opinion, they had hired a CISO without consulting with me about writing the job description or even being part of the interview process. Red flag number one.

"When I met the new CISO for the first time I was impressed by their attitude and enthusiasm to pitch in and help me, as we were educating the legislature, crafting statewide security policies, and realigning statewide procurement of security products and services. Once again, however, I remember having a strange feeling that this person didn't seem to really have the kind of experience you would expect for someone taking over the security and privacy responsibilities of a fairly large organization. Red flag number two.

"We developed a pretty good rapport and began speaking once or twice a week when one day several months later I called this CISO but they were out of the office. I left a message to call me back. A week later I hadn't received a call back so I called again and left another message. Another week went by and no call back so I walked over to the agency and asked a receptionist about the CISO. My antennas immediately began wagging when the receptionist appeared nervous and I could

tell they didn't want to talk to me. This was truly odd and . . . red flag number three.

"I walked back to my office and set up an appointment to meet with the agency head. As I walked into their office the following day, I could immediately tell something was askew. The agency head told me in an extremely embarrassed tone that the CISO was no longer employed there. Of course I was shocked and employed my best negotiation skill of sitting quietly, saying nothing, and waiting for them to talk. The rest of the story was slowly revealed.

"In their haste to hire a CISO, this agency had posted a job description, interviewed candidates, and hired a CISO – all without ever conducting a background investigation. Several months after hiring the CISO, a law enforcement organization met with the agency head and informed them that their new CISO had just been released from prison after serving a term for embezzlement. The CISO job was their first employment following a multiyear prison term. The agency head was personally mortified telling me this story and I can only imagine the look on my face as I heard the tale. They kept saying how embarrassed they were since I had offered to help them with hiring a CISO and they simply forgot in the urgency of filling the role.

"This is easily one of the most extreme examples I've been involved with where a simple background check could have eliminated a serious headache, but it is also one that taught me a good lesson. Not checking all the boxes during a critical process like hiring can be very painful."

No doubt, Mark's story highlights that building the right team to lead the overall cybersecurity program is a complex, difficult challenge. Beyond the CISO, most midsize and large organizations employ managers and/or directors to lead cybersecurity incident response and coordinate with the wider emergency management team throughout the enterprise.

We cover much more about this in Chapter 4.

FREQUENT RANSOMWARE ATTACKS PROMPT RESPONSE CAPABILITY ENHANCEMENTS IN NEW YORK STATE

One thing that Dan learned from his high school football coach is that you can't keep doing the same things over and over and expect a different outcome or result. This concept has proven to be true within the cybersecurity community over the past decade, with the frequency and significant impact of ransomware attacks forcing changes to the strategies and tactics of incident response teams all across the globe. One set of ransomware stories, and how organizations adapted, comes from the former CISO for New York State government.

Deborah Snyder is a senior fellow at the Center for Digital Government, and she has a distinguished career in cybersecurity, most notably as the CISO for New York State until her retirement in late 2019. Deb has a wealth of helpful stories regarding cyber incident response with many practical implications. Specifically, she shared the following ransomware stories.

In the early hours of Sunday, April 9, 2017, Erie County Medical Center (ECMC), a 550-bed hospital in Buffalo, New York, was hit by a cyberattack. Staff noted a digital ransom note on a hospital workstation that demanded $44,000 in Bitcoin cryptocurrency for the key to unlock the hospital's files. Hackers had encrypted ECMC's data, impacting over 6,000 hospital computers.

When a ransomware attack hits a healthcare provider and brings down their computer systems, it can cause significant and life-threatening disruptions, interfering with patient care and public safety. The attack caused ECMC to shut down email and their website, and resulted in a six-week electronic health records systems outage. To avoid further damage, ECMC was forced to revert to paper records and process patient admissions, prescriptions, and other tasks manually for weeks. The FBI investigated, and a cybersecurity firm was brought in to support forensics and recovery efforts. The New York Office of Information Technology Services (ITS) and Cyber Incident

Response Team (CIRT) staff provided security guidance and support to the state department of health in protecting state systems and assets used by the facility. This incident was a wake-up call for many, as it dramatically highlighted the implications of interconnected systems and third-party access, and helped everyone involved grasp the serious potential for collateral impact. While ECMC didn't pay the ransom demand, the massive cyberattack came with a hefty price tag – nearly $10 million in hardware, software, response assistance, overtime, and other related expenses.

In another event, on August 30, 2017, the New York State Cyber Command Center (CYCOM) received a call indicating that Schuyler County had fallen victim to a sophisticated ransomware attack. The New York State CIRT team was immediately activated and an investigation confirmed that the attack involved SamSam – the same variant of ransomware ECMC had experienced. SamSam is typically distributed by compromising servers and using them to move laterally through the network to compromise additional devices. Given the touchpoints between state and county governments – both technical and programmatic – the government temporarily shut down network connectivity and access to the state's network and applications to prevent potential damage. Disruption to the county's 911 center and resulting risk to public safety was a major concern. This incident illustrated the potential for cyber events to have significant impact on public safety operations – fire, emergency medical, law enforcement, emergency communications, and other public safety partners – which in turn would directly and negatively impact the health and safety of the communities they serve. Fortunately, while some enhanced functions, such as integrated mapping, were impacted, the county was still able to receive and dispatch calls.

These incidents, along with the September 2017 Equifax breach that compromised personal data of 143 million Americans, including 8 million New Yorkers, served as a catalyst for formalizing comprehensive cyber disruption protocols. Coordinating resources, reporting, and response efforts across all involved state agencies – the

Office of Information Technology Services, Intelligence Center, and Division of Homeland and Emergency Security Services – enabled better defenses against cyber threats, protected citizens and government assets, and assured a coordinated, whole-of-state response to cyber incidents.

LIKE A BAD PENNY

From 2018 through 2019, ransomware attacks continued to accelerate in number and sophistication across the United States, targeting hospitals, state and local governments, and schools, causing major operational disruptions and financial impact. New York was not exempt.

On Saturday, March 30, 2019, the government cyber response team received a call from the City of Albany, which had experienced a major ransomware attack. Servers and workstations had been encrypted, resulting in significant operational impact across multiple systems and services. The attackers were demanding payment in Bitcoin to unlock systems. The City had engaged law enforcement, and FBI investigators were onsite. Within 30 minutes, the Cyber Command Center CIRT team members were onsite, helping City IT staff and the FBI with critical response actions and forensics.

City officials coordinated response and communications as the investigation and recovery efforts unfolded. The complex interdependencies between systems, data, critical functions, and services that incidents reveal never fail to amaze. Fully understanding these connections and program touchpoints in advance is critical, including linkages to county and state agencies' systems, potential collateral impact on program services, and related third-party dependencies.

New York's comprehensive whole-of-state cyber response protocol ensured coordinated state response efforts across state agencies. Emergency management alerted and assisted state agencies, such as the Department of Health, with connected systems and business processes and the impact on vital records. Routine executive briefings

and the rapid exchange of information assured updates and sharing of available cyber threat intelligence with executives and participating agencies, including the New York State Intelligence Center, Division of Homeland and Emergency Security Services, and the Multi-State Information and Analysis Center (MS-ISAC).

While the attack temporarily disabled some city systems, backups of critical systems enabled recovery, and no ransom was paid. Reportedly, costs associated with remediation and recovery were roughly $300,000, for hardware, software, insurance, and other measures to increase the security and resiliency of the city's systems.[2]

In August 2019, the *New York Times* reported that more than 40 municipalities were victims of cyberattacks – from major cities such as Baltimore, Albany, and Laredo, Texas, to smaller towns including Lake City, Florida, one of the few cities to pay the ransom demand – about $460,000 in Bitcoin – because it determined that rebuilding its systems would be even more costly.[3]

EDUCATION SECTOR TARGETED BY CYBERCRIMINALS

It was Thursday, July 25, 2019, the day after Louisiana's governor declared a state of emergency following ransomware attacks on multiple public school districts in their state.[4] It was near the end of a particularly busy week, when the CYCOM hotline rang – never a good thing, as it generally meant that summer weekend plans would be replaced with handling an active incident.

New York's CIRT team responded to a call from the IT director of Lansing High School in Ithaca, reporting the presence of Ryuk ransomware on the school's IT infrastructure. The next call came from the school district in Watertown. They too had suffered a ransomware attack. A similar attack crippled the Syracuse city school district's computer system. Over the next days and weeks, calls were fielded from multiple school districts across New York State.

The Rockville Centre school district on Long Island was hit with Ryuk ransomware. They later paid almost $100,000 in ransom to restore their data; the school's insurance policy covered the payment. The same ransomware hit a neighboring school district in Mineola. They were able to restore data from backups taken offline over the summer and to rebuild the network.

The New York State Education Department notified all districts about the cyberattacks and coordinated the response to the incidents in affected educational agencies with the assistance of the State Office of Information Technology Services, CYCOM, and other state cybersecurity teams, including the State Intelligence Center, Division of Homeland and Emergency Security Services, and the Multi-State Information and Analysis Center (MS-ISAC). Briefings with the New York State Department of Education and 11 Regional Information Centers (RICs) ensured that everyone had current information and focused support. The attacks were investigated, and the affected agencies recovered and implemented processes to mitigate recurrence.

All told, the New York State Department of Education reported that 16 school districts and one Board of Cooperative Educational Services (BOCES) had been compromised with ransomware.[5] As a precaution, the Education Department directed its regional information centers and big five school systems – Buffalo, Rochester, Syracuse, Yonkers, and New York City – to take the state's data warehouse offline to scan for malware and vulnerabilities.

The state's cohesive cyber disruption and incident response protocols worked well, enabling coordinated analysis and reporting and communications – essential in dealing with multiple and fast-moving attacks. A big win in this particular situation was a tool the CYCOM team developed to identify compromised domain controllers. Based on intelligence and high-confidence observations drawn from onsite and forensics analysis across multiple incidents, the team identified a consistent step in the multiphase attack taxonomy – how attacks unfold and work. Detection and intervention at this critical point in the sequence

effectively disrupted the launch of damaging ransomware. The tool was shared with the Education Department, RICs, state universities, and other government entities to help proactively detect and defend against further attacks.

THE BATTLE CONTINUES

In 2021, adversaries upped their game with more sophisticated tactics and ambitious targets. As government organizations reeled from the impact of a global pandemic, the timing was ripe for another banner year for well-resourced cyber criminals and ransomware. One industry report, "The State of Ransomware in the US: Report and Statistics 2020," noted that 2,354 local governments, healthcare facilities, and schools were impacted by ransomware attacks in 2020.[6] For cyber criminals, government organizations pose an attractive target because they are often resource-constrained and maintain lots of valuable information such as Social Security numbers, birth and medical records, and financial account details. Faced with disruption of essential services to the public, government agencies are often faced with a tough decision – pay or try to restore their systems on their own.

On Christmas Day, 2020, the Albany (NY) International Airport was subject to a ransomware attack, and later paid a ransom to restore access to their data. The ransomware, attributed to a Russian threat actor, had spread to the airport's servers and backup servers from a managed service provider's systems. While the incident reportedly did not impact airport operations, TSA or airline computers, or expose sensitive data, it illustrated the need for organizations to exercise vigilance in protecting against such attacks and manage third-party/supply chain cyber risk exposure.

Some of the top takeaways from these New York State incidents include the importance of good cyber hygiene, due diligence, vigilance, and resilience. Keeping systems patched/current, secure design and configurations, access management – strong identity verification,

authentication, and tightly managed privileged accounts, security awareness training to help users recognize phishing emails and other forms of social engineering, continuous monitoring and detection capabilities, solid backup and recovery platforms that assure rapid restoration of critical systems, and other protections can dramatically reduce the likelihood that ransomware will impact your organization's operations.

FIVE TAKEAWAYS

Shao Fei Huang, CISO of Singapore Land Transport Authority, highlighted his top three takeaways for business owners, board directors, and executives, and the stories from Mark Weatherford and Deb Snyder inspired the last two.

The World Will Never Be Immune to Cyberattacks

Organizations and businesses need to ensure that their cybersecurity strategies are centered on people, process, and technology. Traditionally, the focus has been on IT, and even CISO appointments have been given to the IT staff, reporting to the CIO. Aside from this reporting line, which would result in a conflict of interest, it is key for CISOs to carry a large responsibility in the organization and to be given the authority to raise the alarm if something is not right, even if this relates to the actions of their executives or their decisions.

In appointing CISOs, CEOs and boards should ensure that the individual is equipped with qualities such as strong technical expertise in cybersecurity, business acumen, crisis management skills, and a soft skill that has been often neglected: a flair for public speaking, especially to senior executives and stakeholders.

No businesses want to be a sitting duck, which is why it is critical for the CISO leadership to be appropriately identified and strategically placed in the organization. The CISO and team play a huge role

in steering and executing the cybersecurity program, ensuring that appointed parties are responsible and accountable. The cybersecurity function (ideally led by a CISO) has to be deliberated at the C-suite and reported at the board level.

Cybersecurity Is a Business Risk Issue

More and more people are coming to the realization that cybersecurity is not just an IT issue. The onslaught of recent cybersecurity supply chain attacks and identity breaches on a global scale is a clear sign that it is not a matter of if, but when, an organization discovers it has undergone a cybersecurity attack, whether directly or indirectly. Boards and executives need to understand the "system" at play in how these attacks and the damaging downstream consequences pan out. They do not just center around the IT departments of their organizations, but impact every member within the organization and externally, including each of their customers.

How the organization reacts, responds, and learns from cyber incidents is very much a reflection of the organization's values and capability.

The Double-Edged Sword of Zero Trust

CEOs and boards need to understand what zero trust is and how blindly adopting zero trust could stand in the way of effective incident response (IR) when cyber emergencies happen. The zero trust approach, by definition, is to "never trust, always verify."

The concept is not about making a system or network trustworthy. It is about eliminating trust from the decision loop. While useful as a broad cybersecurity concept, boards and executives need to carefully apprise the risks that come with such an approach, especially if their cyber response playbooks require the use of a service, software update, or patch that cannot be verified quickly enough to contain the incident. Often it may be useful to identify trade-offs early on in a risk-based

approach and take an approach of pre-verifying "verified" systems, vendors, or partners for situations like this.

Pick the Right Person to Lead the Effort

Mark Weatherford's story highlights the vital need to do your homework when selecting a CISO or other top cybersecurity leaders. Much more on this in Chapters 2 and 4, but it must be emphasized upfront that you need someone accountable for the cybersecurity program with the knowledge, experience, a good understanding of organizational culture, and the authority to get things done.

Beyond background checks and impressive resumes (or CVs), does your CSO, CISO, or other top cybersecurity executive excel at relationships in a 360-degree manner with staff, peers, executive management, clients, and vendor relationships? You can strengthen the leader's effectiveness by surrounding him or her with the right mix of professionals who close gaps in weak areas. Finally, does the CISO's vision of success align with the executive board?

Act and Adjust with Resilience as the Cyber Situation Evolves

The eye-opening stories from Deb Snyder reveal an ability to adapt and remain resilient as cyberattacks grow and become more impactful.

In the next few chapters, we will demonstrate how an effective cybersecurity program with relevant strategies, tactics, plans, and playbooks grew to become best practices and eventually standard practices for cyber defense teams worldwide. Leaders can't wait for a perfect solution and allow indecision in the midst of cyberbattles. Rather, they must act and adapt based on threat intelligence, robust information sharing, and a clear understanding of priorities with the tools available to fully utilize their team's skill sets.