California Management Review

TECHNOLOGY

Getting Cybersecurity Right

by Öykü Işık, Dave Chatterjee, and Daniela Almeida Lourenço

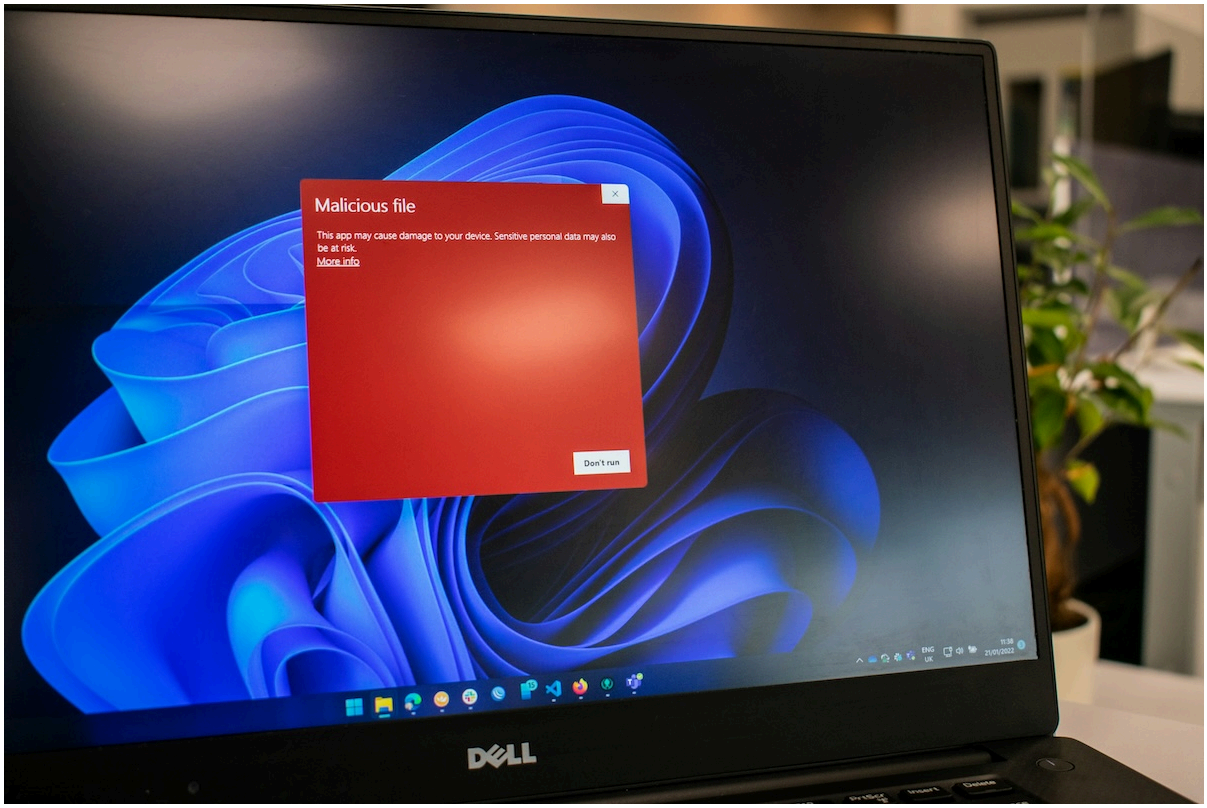

Image Credit | Ed Hardie

Implementing cybersecurity practices isn't enough – you need to ensure they actually deliver.

INSIGHT | FRONTIER 08 Jul 2024

In the fall of 2022, an 18-year-old hacker bought stolen Uber employee credentials from the dark web. Even though they were still valid, multi-factor authentication (MFA) initially blocked the hacker from gaining access to the Uber network – until he posed as a member of Uber's security team. He contacted the employee on WhatsApp and pressured him with a barrage of MFA notifications. The overwhelmed employee eventually gave up and approved one, granting the hacker access and resulting in the data breach. Essentially, the perpetrator exploited what has come to be called "multi-factor authentication fatigue" – a social engineering attack strategy that takes advantage of authentication over push notification, thus exploiting a cybersecurity best practice to commit a breach.

RELATED CMR ARTICLES

"The Digital Workplace: Navigating in a Jungle of Paradoxical Tensions" by Olga Kokshagina and Sabrina Schneider

MFA has been praised as a must-have in cybersecurity for some time now. But clearly, implementing it does not automatically reap its benefits. This context raises the question: how does an organization effectively implement cybersecurity best practices, such as MFA?

Our research investigated why some cybersecurity best practices do not add value despite being widely implemented in organizations today. By interviewing over 30 cybersecurity executives and practitioners, we offer insights on the operationalization of five cybersecurity best practices.

1. Cybersecurity Awareness and Training: Are We Doing It Well Enough?

Conducting cybersecurity awareness and training is a well-known best practice. However, the effectiveness of security training programs depends on factors such as sensitivity to humanistic values, frequency of training, and customization.

Create a Culture of Empathy and Enablement

Phishing simulations, a popular cybersecurity training method, involve sending fake phishing emails to employees in a controlled environment. In 2020, Tribune Publishing conducted a phishing simulation campaign that sent a fake email to test whether employees would fall for an attack and click on a link. To get employee attention, the email contained a **false announcement of employee bonuses**. The simulation was launched after a restructuring exercise marked by pay cuts, furloughs, and downsizing, upsetting employees who felt the organization was using sensitive matters to test their vulnerability. The campaign backfired, and employee discontent was made public through social media, forcing Tribune Publishing to apologize for its lack of sensitivity.

In contrast, a cybersecurity practitioner shared a positive anecdote about an employee who clicked a link in an email she regularly received from a business partner. After learning that the partner had been compromised and the email was a phishing attack, she immediately reported the incident to her organization's cybersecurity team. The prompt reporting enabled the incident response team to act swiftly. The cybersecurity team decided to publicly recognize and reward the employee for her honesty and promptness. This not only set expectations but also helped change the organizational security culture from one of fear and punishment to one of empathy and enablement.

If organizations insist on promoting a culture of fear by blaming employees for their mistakes, instead of helping them become an important part of the cybersecurity defense system, employees will remain a major source of risk. Conversely, when an organization creates a culture of enablement by educating and training its members, those members

feel valued and responsible, motivating them to protect the organization. It is crucial to be sensitive to human values and feelings when creating and conducting cyber training exercises such as simulated phishing attacks.

Commit to Continuous and Customized Training

Instead of a one-shot, once-a-year training, organizations should commit to continuous learning in small increments. With numerous online training courses available, often for free, it should be a no-brainer to review and include them in the security training program.

While general awareness programs are standard practices, good training should be customized to roles and functions. This is especially important for IT and Finance areas, the primary targets of social engineering. An incident response expert lamented that often "IT domain administrators managing critical infrastructure haven't received any training for the last 25 years." He emphasized the importance of IT operators staying updated on the latest security features and configurations of the systems they manage. In his words, "I'm not talking fancy week-long courses, but maybe a two-day course or an online course. Leading vendors such as Microsoft have great online training for free. There's no reason not to set aside just an hour or so for regular learning. Even basic training where you learn about the new features of the server you're using goes a long way."

Creating a cyber-supportive organizational culture through empathy is essential to achieving a high level of preparedness through customized, continuous, and immersive training.

2. Compliance: Going Beyond Ticking the Box

Complying with information security regulations and frameworks is central to cybersecurity governance. While compliance may be necessary for doing business, it may not be sufficient to achieve long-term cyber governance maturity and stability. The story of the RMS Titanic serves as a grim reminder that regulatory compliance does not guarantee safety or security. Despite having prepared 24 lifeboats - four more than required by the British Board of Trade - when the famous ship sank in 1912, the 24 lifeboats were still not enough, and over 1500 people died.

Regulations arise from determined studies and impact analyses and come into force after a lengthy process. By the time regulations are transposed and enforced, reality may have changed – in the case of the Titanic, the construction of a ship of that size was not common, and there was no historical data to support more stringent controls. This lag between the need for control and the resulting regulations is usually more evident in scenarios posing a direct public health risk, such as the delay between the first conclusive studies on the health hazards of asbestos in the early 20th century and the legislation enacted to progressively control its use until it was finally banned many decades later. The general public knew that asbestos was life-threatening; however, organizations and states took their time (in line with the regulations) to comply just-in-time with the regulatory provisions.

Approach Compliance Requirements as a Guide to Best-of-Class Controls

What makes cyberspace more sensitive to this lag is the tendency of technology to develop and change at hyper-speed. Take the **European Union (EU) AI Act** – it took almost three years to develop, and by the time it was approved, the way organizations used AI had completely shifted. Meanwhile, other regulations such as the NIS2 Directive, the Digital Operational Resilience Act (DORA) in the EU, or the 2023 Security and Exchange Commission (SEC) final rule for cybersecurity in the US are being enforced to improve maturity at scale. Consequently, cybersecurity vendors emphasize compliance in their marketing, risking the prioritization of compliance over solving real organizational problems.

Going Above and Beyond the Minimum Compliance Requirements

It is imperative that organizations adopt a substantive approach to compliance, moving beyond a "tick-the-box" mentality and instead committing to meeting and exceeding expectations. Here are some instances of meeting and exceeding compliance requirements:

- Monitoring and gathering cyber intelligence is a good practice; it checks the box for security monitoring requirements, but prompt processing and decision-making based on intelligence received is what sets an organization apart. An exemplary

organization will document the intelligence received, the decisions made, and the rationale underlying the decisions.

- A lengthy security update email to the organization might check the communication compliance box. However, for security communication to be effective, it must be concise, customized, and supported by feedback mechanisms that ensure the message has been received by the targeted recipients and interpreted as intended. Submarine personnel in the US Nuclear Navy are required to repeat verbatim the command instructions of their supervisor before executing them.

- Implementing strong access control measures is another requirement of standards. Regular testing of the existing control mechanisms, reporting on the findings, and taking prompt action to address identified vulnerabilities would set apart a proactive security-conscious organization from those that tend to be only reactive.

Organizations can foster a high level of preparedness by going above and beyond regulatory requirements; compliance should be seen as a confirmation exercise, not the actual goal.

3. Breach Notification: Communicating the Right Thing at the Right Time

Despite the increasing volume of breaches today, most organizations handle the communication aspect of such incidents shortsightedly. The case of Uber's ex-CISO Joseph Sullivan is a good example; in May 2023, **he received a three-year probation** sentence for his involvement in concealing a cyber-attack from authorities. Sullivan was convicted for his role in paying hackers $100,000 to keep quiet about their unauthorized access to 57 million Uber customer records containing personal information such as names and phone numbers.

As damaging as hiding a data breach incident may be, not properly communicating to the affected parties can have even worse consequences. When Travelex, the currency exchange platform, was breached in 2019 with ransomware, the CEO chose to wait several days to issue a first public message and only announced that the company was undergoing

planned maintenance. Following customer outcry and countless social media posts of travelers unable to access their money, Travelex finally made another public announcement explaining that a software virus was impacting its services.

Like Travelex, many senior leaders would prefer to keep breaches secret, fearing reputational damage. However, that is no longer an option for publicly traded US companies. The recent SEC ruling mandates that publicly traded companies reveal the attack incident's nature, scope, timing, and impact, "within four days of identifying that it has a 'material' impact on their finances." The disclosure may be delayed by an additional period of up to 60 days "should it be determined that giving out such specifics would pose a substantial risk to national security or public safety."

Below are the key elements of effective breach communications:

Don't Rush to Communicate

Seek the expertise of incident responders before communicating incident details. According to a subject matter expert, most often the bad thing shows up last. In his words, "… it never shows up as the flashing light in the beginning." It takes time to establish necessities such as IP addresses and servers, and it's never easy to identify data exfiltration. If the affected organization communicates too early and suggests no data has been breached, they may end up withdrawing those early statements. Later, when evidence of data exfiltration is found, reputational damage becomes unavoidable. That is why communicating too early, without analysis results in hand, is a mistake many incident responders warn against.

Be Honest and Transparent

Leadership must be honest and transparent when communicating with relevant stakeholders. Clearly articulate what happened, why it happened, the potential consequences, and the action plans for recovery.

Norsk Hydro's response to their breach is a good example of honest and transparent communications. After being breached by ransomware in 2019, the Norwegian aluminum company had to shut down several production plants. Despite the incident's impact, Norsk

Hydro responded with transparency and demonstrated resilience by promptly informing stakeholders and implementing robust incident response measures. The company focused on restoring its systems, enhancing cybersecurity measures, and minimizing the long-term effects of the attack. As a result, they managed to gain the public's empathy and understanding, even receiving the Norwegian Communication Association's Transparency Award.

4. Hiring a CISO: Are They Empowered to Succeed?

The role of the Chief Information Security Officer (CISO) is crucial for cybersecurity governance and accountability. Hiring a CISO and making them accountable generally signals that the organization is serious about cyber governance. Today, there is growing recognition that CISOs are business enablers and can play a key role in making risk-aware strategic decisions. An effective CISO will find ways to enable strategic initiatives by guiding organizational members to conduct them securely. According to a CISO we interviewed, CISOs are not supposed to be naysayers; they must engage with the business and ensure they understand the cyber risks associated with their activities and processes. However, with the increasing volume and frequency of breaches, CISOs can end up becoming scapegoats and are under more stress than ever. Most organizations that have a CISO assign them many responsibilities yet do not equip them with the resources and necessary decision power to accomplish these. In a high-performing information security culture, CISOs have responsibility and authority. Below are guidelines to help executives ensure this balance:

Avoid Conflicts of Interest

Organizations may face conflicts of interest scenarios that arise from CISOs reporting to CIOs or CTOs, instead of reporting directly to the Board. Regardless of any formal compliance charter, many CIOs may still see security as a showstopper, and there may be occasions where the priorities of the CISO clash with those of the CIO. For instance, to mitigate the risk of insider threat and the rise of vulnerabilities, the CISO may plan to implement separation of duties procedures and software development and deployment

security controls, but the time-to-market pressure on the CIO might cause rejection of the CISO plans. The CIO may even underestimate the risks identified by the CISO and unilaterally decide not to inform broader management about them.

Empower Your CISO with the Right Structure

To be effective, the CISO function must be suitably structured and empowered. The reporting relationship should be such that the CISO can objectively alert the organization of potential threats and vulnerabilities. According to cybersecurity practitioners we interviewed, it is better to make the CISO independent of the CIO and elevate the CISO to a level where they can drive the mandate of cybersecurity. The more elevated and empowered the CISO, the more committed their mission to cybersecurity will be. If a CISO reports to somebody three levels below a CIO, they will not be able to make a difference; even if they are highly capable and competent, the organizational structure will block them from performing effectively. **The CISO must report to the most powerful person** in the organization to get the right resources and sponsorship.

5. Threat Intelligence: Gathering and Using it Properly

There are several reported instances of organizational inaction in response to threat intelligence. British Airways (BA), the flagship airline of the United Kingdom, suffered a major data breach in the summer of 2018. According to the Information Commissioner's Office (ICO), a hacking group called Magecart exploited a Javascript vulnerability on BA's payment processing website and app. They were able to divert passenger data to a similar-sounding rogue site named baways.com. The personal data of about half a million passengers were compromised, including names, addresses, contact information, and payment card details, including the three-digit security code.

According to security experts, the vulnerability was well-known, and it was surprising that BA had not updated their script since 2012 when the vulnerability became known. Effective monitoring would have revealed the weakness, and BA could have averted the

major breach. Even more disconcerting is that BA hadn't fixed the problem even after a year of the attack.

Do Not Let Actionable Intelligence Get Lost in the Noise

There are probably numerous other unreported instances of slack cyber incident responses. This lack of preparedness is likely due to several factors, such as:

- Numerous alert sources that cause alert fatigue.
- Security operations center (SOC) personnel overloaded with numerous cases of false positives.
- An information security workforce that is not well-organized.
- Unclear accountability models, where the vulnerabilities or events are visible, but the respective corrections or patches (which potentially demand resources and downtime to be implemented) are pushed from one department to another, creating a technocratic limbo.

Meticulous and Prompt Processing and Logging

Organizations need to go back to the drawing board and embrace a disciplined approach to cyber intelligence monitoring and processing. This process entails:

- Identifying intelligence needs – what they want to know if something goes wrong and where.
- Identifying credible intelligence sources – shortlisting and approving credible information sources.
- Establishing processing and logging mechanisms – forming a team and instituting a reporting structure to review and meticulously log credible threats and recommended actions.
- Putting in place a highly trained SWAT team ready to act on short notice.

In summary, we recommend organizations commit to a proactive and thorough approach to threat intelligence processing and action. Such preparedness will serve organizations well not only in the court of law but also in the court of public opinion.

There is no shortage of guiding frameworks and recommended best practices in cybersecurity. However, there is often a gap between cybersecurity actions and intentions. Most top management teams, despite realizing the urgency in implementing cybersecurity, fail to understand the need for structural commitment and resources, two fundamental keys to delivering long-lasting benefits. The practitioners we interviewed emphasized the value of a comprehensive line of action to enable such understanding. To build resilience in organizations, leadership teams need to foster a holistic approach to cybersecurity that goes beyond a simplified implementation of best practices.

Öykü Işık Follow

Öykü Işık is Professor of Digital Strategy and Cybersecurity at IMD in Lausanne, Switzerland. Her research and teaching focuses on digital resilience. She has been recognized as a Thinkers50 Radar thought leader in 2023, and serves as a member of the WEF Global Future Council on Cybersecurity.

Dave Chatterjee Follow

Dave Chatterjee is Associate Professor at The University of Georgia and Visiting Scholar at Duke University. He authored the book Cybersecurity Readiness: A Holistic and High-Performance Approach. Dr. Chatterjee has written scholarly papers, consulted with companies, and delivered numerous talks worldwide and hosts the Cybersecurity Readiness Podcast Series.

Daniela Almeida Lourenço Follow

Daniela Almeida Lourenço is an information security practitioner based in the Netherlands. She holds a Master's Degree in Communication and Cultural Studies and an Executive Master's in Cybersecurity. She is CISM, CISSP, C|CISO certified and she is currently the CISO for a financial services organization, and collaborates with ISACA's Netherlands Chapter.