Magazine

Preventing security breaches must start at the top

by Dave Chatterjee Published 28 September 2022 in Magazine • 10 min read

Technology alone will not stop successful cyber criminals attacking your company. C-level executives must lead the way in planning, implementing and monitoring

effective security initiatives.

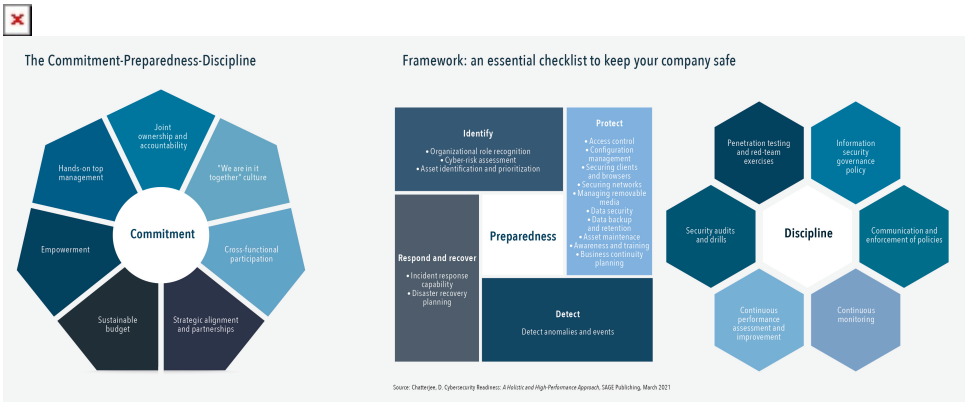
Cyberattacks are increasing in number and growing in sophistication. Organizations must develop a comprehensive plan, executed with great precision and consistency, if they are to protect themselves. The creation and sustenance of a high-performance information security culture is needed, and the drive for change must come from the very top. In my book *Cybersecurity Readiness: A Holistic and High-Performance Approach*, such a culture is characterized by three key traits: commitment, preparedness, and discipline.

This Commitment-Preparedness-Discipline framework (see the charts below) is holistic and recognizes that “technology alone will not mitigate information security risks”.

There are several pieces to the complex puzzle of cybersecurity management, and technology is only one of them. Committed leadership, robust governance procedures, informed and motivated personnel are other success factors.”

Sustained commitment at all organizational levels and beyond (value chain partners), coupled with a rigorous approach to securing data, network, locations, people, and storage devices, and the discipline of meticulous planning, sound execution and continuous monitoring, are the cornerstones of an effective cybersecurity governance program.

Each of the information security cultural traits of commitment, preparedness, and discipline, are associated with several success factors. In this article, I focus on “Hands-On Top Management”, not only due to its innate significance, but also because senior leadership can play a significant role in enabling the realization of other success factors.



The Commitment-Preparedness-Discipline

Hands-on Top Management

This implies active participation and involvement of C-level executives in cybersecurity initiatives, including planning, execution, monitoring, training, assessment, and review.

In exemplar organizations, members of the senior leadership team are known to serve on governance and oversight teams and committees. They continuously strive to stay abreast of the organization's vulnerability points and defense mechanisms, actively engage in cybersecurity strategizing, take ownership and responsibility for cybersecurity investments and actions; and champion and evangelize the importance of cyber preparedness throughout the organization.

Other recommended best practices include: a) the state of cyber readiness consistently featuring as an important agenda item in top management meetings; b) regularly briefing the

board on the state of preparedness; c) participating in training sessions and workshops; d) engaging in cyber defense simulation exercises; e) introducing incentives and rewards to motivate adoption of the desired cybersecurity behavior; and f) adopting suitable measures and metrics to track and monitor performance.

Is it a tall order to expect the senior leadership to treat cybersecurity readiness as a core competency and an integral part of an organization's value propositions ?

Is it a tall order to expect senior leadership to treat cybersecurity readiness as a core competency and an integral part of an organization's value propositions? Should CEOs need much convincing in actively engaging in cyber governance? Not really, if you asked Rohit Verma, the CEO of US-based insurance firm Crawford & Company. In a podcast interview, Rohit said that "if the leadership of other organizations needs any convincing about staying up with cyber training, all they need to do is look up the *Wall Street Journal* for the last three months and read about the extent of havoc cyberattacks can cause an organization". He added that "several of us in senior

leadership are digital immigrants and not digital natives. Many of the security issues are new to us. We will be naïve if we don't take interest and are not willing to learn and stay updated".

A review of major breaches from 2013 to 2019 brings to light alarming instances of vulnerabilities and shortcomings that can be broadly classified under negligence and lack of preparedness.

It is incumbent on the senior leadership to try to ensure that such glaring security lapses never happen. They need to work closely with the legal team to ensure that due diligence standards are not only met but exceeded. While compliance with regulatory requirements are important steps in the right direction, exemplar organizations and their leadership will go above and beyond in making substantive efforts to protect sensitive assets.

When top management is proactive in adopting robust security measures and does so because it is the right thing to do — and not because there is a legislative requirement — then that's when they have taken a huge leap forward in establishing a high-performance information security culture. In the event of a successful attack, they can say to their stakeholders and the public at large that they left no stone unturned, and made every reasonable effort to prepare. Such organizations and their leadership are likely to be viewed and treated fairly, whether in a court of law or the court of public opinion.

The good news is that over the years surveys and research reports reveal a marked improvement in how top management has started viewing cybersecurity readiness.

There is greater realization that information security management can be a core competency and a source of competitive advantage. A cybersecurity thought leader said it best: “Most people think about security as avoiding a bad thing. Let’s not get hacked. That is a good way to think about security, but it’s incomplete. We need to think about not just how do we avoid a bad thing, but also how do we get a good thing? Not just how we do not get hacked, but how can we gain an advantage?”

10 acts of negligence and lack of preparedness

Usernames and passwords not encrypted.
A weak encryption system.
Unencrypted customer data stored in multiple locations.
Networks not adequately segmented.
Multi-factor Authentication (MFA) not in place.
Delay in notifying victims.
A breach goes undetected for several weeks.
Company fails to heed alerts sent by monitoring company.
Web application firewall is misconfigured.
A lack of well-rehearsed disaster recovery and incident response plan

Senior management’s enabling influence on other success factors

A highly motivated and engaged top management can play a significant role in helping achieve several of the other success factors associated with creating and sustaining a high-performance information security culture. Here are six steps to get right:

1. Building a culture of ‘we’re in it together’

By “walking the talk” and actively participating in cybersecurity readiness activities, senior management can help to build and sustain a highly involved culture where all members of the organization are emotionally invested and have bought into the fact that cybersecurity readiness is everyone’s business, and that they all have an important role to play. As I write in my book, senior leadership can help build emotional capital, a key ingredient for fueling a “we’re in it together” culture, “by creating a work environment where employees: a) feel valued and develop a sense of belonging; b) take pride in their work; c) are having fun; and d) perceive leadership to be genuine and authentic”.

Marcin Ganclerz, a cybersecurity awareness and training specialist, emphasizes the importance of creating such a cohesive culture. Referring to it as a culture of enablement and not fear, he said: “When you have this culture of fear, employees don’t want to report any suspicious email; they are afraid of making mistakes because you blame them for the mistakes.”

2. Empowering the role of CISO

The effectiveness of the CISO role and function often depends on the extent of C-level support and commitment, as well as being able to operate with a high level of independence and objectivity. According to Vishal Salvi, CISO and Head of Cyber Practice at Infosys, the CISO needs to deliver on his or her agenda to gain trust and credibility. He also believes that the CISO’s ability to meet and exceed expectations also depends on the reporting structure. “Make the CISO independent of CIO and elevate the CISO to a level where they are able to drive the mandate of cybersecurity,” he said. “The more elevated and more empowered the CISO, the more committed is the organization’s mission to cyber.”

Whether the CISO reports directly to the CEO or to an independent external committee (such as the board of directors or audit committee) is a decision that can be significantly influenced by top management. In addition, by recognizing the CISO role to be that of a strategic enabler and

involving them in strategic decision making, the senior leadership team is likely to be more effective in risk-based prioritizing of projects and initiatives.

3. Ownership and responsibility must be shared

In addition to appropriately empowering the CISO function, there needs to be cross-functional ownership and accountability of cyber risks and breaches. Top management can enable this governance approach by requiring that every cybersecurity project and initiative has a business owner and sponsor. Even in the case of outsourcing of security services, top management should mandate a rigorous vetting and selection process followed by close monitoring of vendor performance. Service level agreements (SLAs) should be suitably crafted to ensure that third-party service providers have “skin in the game”, and work closely with their clients and customers to protect data stored on their servers.

Such due diligence is essential to mitigating the risk of data breaches caused by vendor negligence and inadequate monitoring and oversight by client organizations.

4. Awareness and training

It is standard practice, often mandated by regulations, that organizations require all of their stakeholders to participate in cybersecurity training programs and workshops. For such training to be truly effective, it must be customized and personalized.

Depending on their roles and responsibilities, employee skill and awareness level need to be suitably enhanced. Immersive training methods involving gamification and a hands-on approach is more effective than the standard approach of watching videos and demos and then responding to a set of questions.

Another best practice is to offer continuous skilling and re-skilling opportunities and incentivizing the commitment to learning. Like Wordle and Nerdle, the daily word and mathematics games and challenges, organizations can adopt an incremental, continuous approach to spreading security awareness and knowledge. Senior leadership should encourage and evangelize innovative and substantive approaches to information security training. They need to ensure that this very important preparedness mechanism does not degenerate into a check-the-box exercise.

5. Prompt processing of threat intelligence

A variety of intelligence tools and resources are at the disposal of organizational teams focused on gathering and processing threat intelligence. The challenge lies in the prompt processing of alerts and taking prompt action.

Organizations are often found wanting in the ability to follow through on the intelligence received from external sources. For example, a 2017 hack at Equifax, a credit reporting agency

that exposed the personal data of nearly 150 million people, could perhaps have been avoided if management had acted quickly on the intelligence received.

It is imperative that suitable governance structures and procedures are in place to ensure that threat intelligence alerts are properly logged and acted upon. The rationale for a decision to act, or not to act, also needs to be documented. Top management intervention can go a long way in instilling this threat management discipline.

6. Security audits and drills

One hallmark of a highly disciplined information security culture is the continuous review and rehearsing of an organization's information security plan and recovery capabilities. Compliance requirements often mandate the conducting of information security audits and simulated practice exercises to identify and address deficiencies. Top management at exemplar organizations can take this a step further by requiring real time and continuous security audits and conducting extensive information security drills.

> **"Like Wordle and Nerdle, the daily word and mathematics games and challenges, organizations can adopt an incremental, continuous approach to spreading security awareness and knowledge"**

Audits are reactive by nature and provide after-the-fact insights. While such revelations are valuable, often they are not timely enough to avoid disasters. So, the practice of creating audit teams that continuously engage in identifying and reporting on security vulnerabilities is a step in the right direction. It is relatively standard practice for organizations to engage third-party service providers to test the various technical controls. But organizations need to go beyond regular penetration testing and expand the scope of the real-time audits to include a thorough review of administrative and physical controls. Top management also needs to ensure that the audit report findings are being promptly reviewed and acted upon. The findings and actions taken must be documented and regularly reviewed by a senior leadership team.

Conducting periodic fire drills is a relatively common and established organizational practice. Carrying out extensive information security drills to assess an organization's ability to recover from different types of breach scenarios is the next-level practice that marks out a highly security conscious organization. Regularly rehearsing action plans will help an organization to stay at a high level of cyber readiness. It is highly recommended that top management actively engages in, and get others involved in, rehearsing disaster recovery plans under different threat scenarios. The drills need to go beyond table-top exercises and simulate disaster scenarios as realistically as possible.

The dilemma for senior leadership

Since there is no guaranteed immunity from cyber threats and attacks, senior leadership often is at a crossroads when it comes to investing too much time, money, and other resources in reaching a certain state of preparedness. This mindset was evident during a C-level meeting at a

major healthcare organization, where the CEO encouraged the leadership team to focus on the organization's primary mission, i.e., providing quality care, and not wasting time, money and effort on trying to bullet-proof the organization from potential attacks.

Art Ehuan, Vice President of Palo Alto Networks, and a former FBI expert in cybercrimes, effectively articulates this leadership dilemma in the context of dealing

with rampant ransomware attacks: “The CEO is trying to decide, do I put more money into cyber, or do I put more money into customer satisfaction? You know, that’s sometimes a hard decision because you’ve got limited dollars and trying to make that decision is sometimes difficult.”

While the CEO is not expected to be the cyber chief for the organization, his or her active oversight and involvement can make a huge difference and does set the tone for how cybersecurity governance is viewed and practiced.

Authors

Dave Chatterjee

Associate Professor in the Department of Management Information Systems at the Terry College of Business, The University of Georgia.

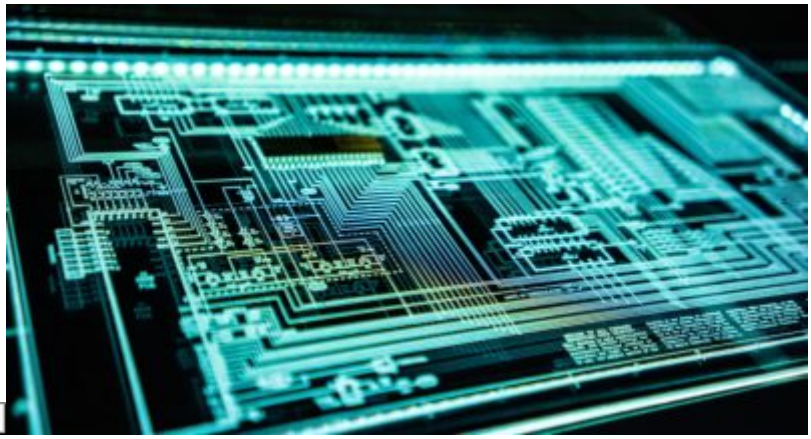
Dave Chatterjee, Ph.D. is tenured (Associate) Professor in the Department of Management Information Systems at the Terry College of Business, The University of Georgia. As a Duke University Visiting Scholar, Dr Chatterjee has taught in the Master of Engineering in Cybersecurity Program at the Pratt School of Engineering. His book, *Cybersecurity Readiness: A Holistic and High-Performance Approach,* was published by SAGE Publishing in March 2021. Dr Chatterjee is also the host of the Cybersecurity Readiness Podcast Series.

Related

Protect and survive: act now on cybersecurity

22 September 2022 • by Öykü I□ık in Magazine

Experts from the public and private sector – including CEOs, board members and government officials – are gathered in Lausanne for the Financial Times' Cyber Resilience Summit, where strategies for overcoming new...



Five ways to plug the gaps in your digital security

15 September 2022 • by Akshay Joshi in Magazine

'Cybersecurity failure' continues to feature as a critical threat, so it is vital that senior leaders get serious about tackling the issue....

The paradox of power: to serve myself or others?

12 July 2022 • by George Kohlrieser in Magazine

Leaders must strike the right balance between their own needs and the needs of others....

Audio available

Drive hard into the future and don’t look back

6 July 2022 • by Howard H. Yu in Magazine

The urge to return to business-as-usual must be resisted. Commitment to change and innovation is more important than ever, explain Howard Yu and his colleagues at IMD’s Center for Future Readiness...

Audio available

Learn Brain Circuits

Join us for daily exercises focusing on issues from team building to developing an actionable sustainability plan to personal development. Go on - they only take five minutes.

Read more

Explore Leadership

What makes a great leader? Do you need charisma? How do you inspire your team? Our experts offer actionable insights through first-person narratives, behind-the-scenes interviews and The Help Desk.

Read more

Join Membership

Log in here to join in the conversation with the I by IMD community. Your subscription grants you access to the quarterly magazine plus daily articles, videos,

podcasts and learning exercises.

Sign up