Strengthening Your Cyber Security Reputation

Strategic Recommendations for CISOs and Cyber Leaders
Table of contents

Introduction

Chapter 1: Anticipate and Manage Risk in Your Cyber Environment

Chapter 2: Discover New Ways to Augment Cyber Risk

Chapter 3: Learn How Gamified Training Enhances Team Performance
  - Elements of Gamification
  - About Project Ares
  - Frequently Asked Questions on Project Ares

Conclusion
CISOs, cyber directors and leaders have a tough job.

They’re responsible for leading teams who help protect their employer from known and unknown vulnerabilities while defending against imminent attacks. Hacker methods are always changing, technologies evolving, and business leaders hyper-focus on increasing efficiency, effectiveness, and productivity across departments—and the CISO or cyber director has to juggle all of that in the context of security.
At the end of the day, reputation is on the line.

If a breach occurs, the CISO has to take steps to not only remediate the risk but prevent it from happening again. That’s a lot of pressure to put on team of cyber professionals, let alone one person – especially when cyber security is integrated into every facet of the business process from employee endpoints to the intricacies of the SOC. It’s not an isolated business function anymore yet the CISO has to ensure everything is protected from any kind of risk.

So how can CISOs strengthen their security reputation in the wake of these challenges? This e-book identifies three core areas to start.
Goal:

Help CISOs and cyber security leaders protect and preserve their professional reputation by leveraging new technologies, measuring elements of security posture against industry standards, and exploring gamified training.

This e-book helps readers:

- Anticipate and manage risk in any-sized cyber environment
- Discover new ways to augment cyber defense
- Learn how gamified training enhances team performance
Chapter 1

Anticipate & Manage Risk in Your Cyber Environment

You can't prepare for threats you didn't anticipate, so performing regular cyber risk assessments are critical. Beyond the standard security maintenance efforts listed here, anticipating and managing risk also means asking the right questions about the security of both your infrastructure and the people using it.
Important questions

- What can a hacker gain access to today?
- What prevention do we have in place and what are we doing to proactively reduce risk?
- How would we know if we were breached?
- Are our air-gapped networks vulnerable to any degree?
- Is there any customer data or sensitive data involved?
- What is the financial impact of a breach?
- How would a breach impact our compliance?
- Do other departments and executives understand the impact and risk of a breach?
Threat Mitigation

- Identify threat sources
- Perform patching
- Conduct vulnerability scans
- Review asset management
- Evaluate access controls
- Revisit incident response plan
- Check security benchmarks
- Determine attack impacts
Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.

— NIST
National Institute of Standards and Technology
Overall security risk

Your cyber environment isn’t defined by the infrastructure alone. It is comprised of you and your team (even if that’s just one other person). And your security is only as strong as your weakest link—and that’s usually people.

There are many ways to calculate risk. If the information is coming from a vendor, trusted security firm, or automated tool, use their risk assessment/severity system in place. If you are working internally to identify risk severity, try the above chart.
Chapter 2

Discover New Ways to Augment Cyber Risk Management

In this day and age with ever evolving cyber threats, it is important to continuously expand our cyber defense strategies by leveraging as much automation as possible. When using automation solutions and tools, the goal should be to reduce the manpower required to monitor and address cyber threats without compromising security. Many companies turn to artificial intelligence and machine learning technology to better support their personnel.
AI helps by automating complex processes for detecting attacks and reacting to breaches. These applications are becoming more and more sophisticated as AI is deployed for security.

– Forbes
There are many tools that help CISOs and cyber leaders automate tasks including intrusion prevention systems (IPS), Firewalls, endpoint detection and response systems (EDRs), and anti-malware software. But we can’t rely on those alone to harden our posture.

When an incident arises, people are still at the helm of response and they need to decide how to properly handle the tools they have with the team they have available.
Keep things simple

Too many tools can cause tech debt, noise, or tend to increase reliance on them for security. While AI can improve existing technologies or offer some unique solutions, remember they are still just a tool to support your cyber team.
Chapter 3

Using Gamified Training To Enhance Team Performance

Traditional cyber training takes place in either off-site classrooms or via online tutorials. Both teach cyber concepts passively, meaning the learner watches or listens to material being delivered and has to absorb it and remember it come exam time.
Gamification is defined as the process of adding games or gamelike elements to something (such as a task) so as to encourage participation.

Merriam-Webster
Elements of Gamified Learning

- Leaderboards
- Realistic scenarios
- Arcade-style games for concept learning
- Battle rooms for individual skill building
- Missions for team-based cyber collaboration
- Cyber ranges for true-to-life network emulation
- AI to challenge player progression and facilitate deeper learning
Benefits of Gamification

Over the years, passive teaching approaches have proven ineffective at helping learners retain information, which is a serious issue if professionals are trying to develop professionally and acquire the latest skills to keep pace with the latest threats. If they can't remember what they've learned in training, they can't apply it to their own cyber situations—leaving organization's security posture in a state of limbo.

Today, gamification is being incorporated into cyber training programs to engage learners better. It's considered an active-learning approach (learn by doing), which studies show increases learner retention rates to 75-90% instead of 5% with passive-learning models.
Project Ares: Gamified Cyber Learning

Circadence's Project Ares® is a gamified, virtual cyber range environment running on Microsoft Azure that allows professionals to train individually and in teams via a browser—so learning can happen anytime, anywhere.
Project Ares: Cloud-Based Scalability

Cloud-based training allows organizations to scale training up or down, left or right and flexible ranges can emulate company networks while trainees use their own tools and techniques to make the training environment as “real” as possible.
The Project Ares AI-powered in-game advisor “Athena” helps trainees progress through activities and act as the automated adversary to challenge players to reach new heights in skill acquisition.

Project Ares: AI-Powered Learning
Activities in the platform are inspired by and based upon real-world threats happening today from the famous WannaCry attack to breaches specific to industries like financial services, water treatment plants and more.

Trainees can select activities that are most relevant for their cyber security environment, so learning instantly becomes more meaningful and applicable to their day-to-day jobs.

CISOs can gauge their team’s performance from the Trainer View and download player reports to see where their team is excelling and where they are falling short—so they can develop plans to strengthen competencies, which in turn, strengthens posture.
Summing it up
There must be balance

By building a risk assessment program that works best for your organization, leveraging AI to augment aspects of human workloads, and gamifying cyber training to keep cyber teams continuously learning, CISOs and security leaders will be better poised to protect their reputations and their company from breaches.

It’s common to misunderstand the reason security measures are put in place—just as it’s easy to misunderstand reasons behind law enforcement. For CISOs, it’s a battle of convincing their colleagues why they need security, especially if they are doing their job correctly and there are no incidents. It’s also easy to put security first and let it become a hinderance to productivity and results.
Circadence® is a market leader in next generation cyber security readiness. Circadence has leveraged its history of software advancement, multi-player game development, and a deep understanding of application optimization to offer Project Ares, the only fully immersive, AI-powered cyber security learning and assessment platform in the market today.

Learn more about gamified cyber training at: www.Circadence.com.