

The Complete Compliance and Ethics Manual 2024

Cybervigilance in Establishing Security Cultures

By Mark Lanterman^{[1][2]}

Given our technological landscape and ever-increasing dependence on interconnected devices, it is an unfortunate reality that where we gain convenience, we lose security. From spear-phishing campaigns that seek to compromise the human element of security to ransomware attacks, organizations are tasked with implementing reactive and proactive strategies to counteract cyber threats and risks.

Cybervigilance is a cornerstone of strong security cultures. Developing a culture of security within an organization requires a combination of proactive and reactive cybersecurity measures, including top-down management support, asset prioritization, well-documented communication channels, incident response planning, regular security assessments, and employee education.

Key Facts

- **Threat actors have four primary motivations for committing cybercrimes**, including financial gain, political and/or ideological beliefs, curiosity and fun, or for some emotional benefit. Financial gain is the most common factor, but organizations may be targeted for any one or combination of these reasons.
- **The typical profile of a cybercriminal goes far beyond the standard vision of a lone hacker** sitting at a computer in a basement. While lone hackers exist, cybercriminals may be hacktivists, organized criminals, or even professional criminals that work for a greater group. Nation states may also be responsible for acts of cybercrime, as demonstrated by the Sony hack of 2014.^[3]
- **Cyberattacks can damage an organization financially, reputationally, legally, and operationally.** The effects of a cyberattack can have both short-term and long-term repercussions that affect overarching goals.
- **As technology and cybersecurity strategies strengthen, so too does a cybercriminal's ability to counteract** with stronger threats. Malware, social engineering attacks, distributed denial-of-service attacks, advanced persistent threats, and brute-force attacks are all ways that an organization may be attacked.
- **Top-down management support is critical in establishing cultures of security** that take a proactive approach to cybersecurity, vigilance, and resilience. "Set it and forget it" security protocols are incapable of effectively addressing the types of threat actors and risks that organizations face on a daily basis.
- **Incident response teams and clear communication channels for reporting cyber incidents help** in relieving the chaos that comes in the wake of a cyberattack, quickens mitigation efforts, and improves public response.
- **Cyber awareness within an organization relies on ongoing investment in security assessments, employee**

training, and education. While top-down support is critical, it must be understood interdepartmentally that cybersecurity is everyone's responsibility.

- Recommendations:
 - Enterprises must incorporate a cyber security approach that takes both reactive and proactive strategies into account.
 - IT security can no longer be the hub of cyber defense communication. Establish a corporate communication initiative that begins with the tone at the top and is administered by risk and/or compliance in partnership with IT.
 - Establish incident response teams that are charged with handling cyber events, including but not limited to public response, internal investigations, external communications, and preliminary mitigation efforts.
 - Act now. Organizations should establish a security baseline via a maturity assessment and proceed from there. Assume vulnerabilities exist and promote an attitude of "when, not if" in regard to potential attacks and breaches.

Introduction

Cybercrime can be incredibly lucrative and relatively low risk, making it an attractive option for criminals on a national and global level. Historically, cybercrime required knowledge of networks, technology, and standard security measures. That is no longer the case. Today there are malware-as-a-service companies that will create worms, phishing attacks, Trojans, viruses, and other malware on demand. Additionally, many individuals work within a group to perform small cybercrime tasks in order to execute a greater attack.

The cyberworld is constantly evolving. Organizations face threats from a variety of angles. Disgruntled employees can seek to disrupt or embarrass the organization or sell company trade secrets. Organized espionage groups can actively look to penetrate databases and steal transactional information. Companies that have, or appear to have, a social agenda face the threat of activist dissidents seeking fame and notoriety for their cause through malicious insertions and denial of service.

The FBI's 2022 *Internet Crime Report* states, "In 2022, the IC3 received 800,944 complaints, which is a 5 percent decrease from 2021. However, the potential total loss has grown from \$6.9 billion in 2021 to more than \$10.2 billion in 2022. While the number of reported ransomware incidents has decreased, we know not everyone who has experienced a ransomware incident has reported to the IC3."^[4] The report demonstrates that phishing attacks remain the most commonly reported event.

In the Executive Order on Improving the Nation's Cybersecurity,^[5] President Biden detailed a roadmap for improving the nation's security posture. This order addresses the need for modernization within the federal government and established the creation of the Cyber Safety Review Board. The purpose of this board is to review and provide lessons learned from major cyberattacks and to promote cooperation between the private and public sectors. In March 2023, the National Cybersecurity Strategy laid out a new gameplan to address the risks of our digital landscape. The Strategy is markedly more proactive than those put forth by previous administrations, and highlights the importance of collaboration, modernization, and resilience.

We will realign incentives to favor long-term investments in security, resilience, and promising new technologies. We will collaborate with our allies and partners

to strengthen norms of responsible state behavior, hold countries accountable for irresponsible behavior in cyberspace, and disrupt the networks of criminals behind dangerous cyberattacks around the globe.^[6]

Other requirements and standards include, but are not limited to, the joint standard of the International Organization for Standardization and the International Electrotechnical Commission, known as ISO/IEC 27002:2022;^[7] the Committee of Sponsoring Organizations of the Treadway Commission standard for cyber risks;^[8] the National Institute of Standards and Technology Cybersecurity Framework;^[9] the Internet Engineering Task Force Site Security Handbook, RFC 2196;^[10] the International Society of Automation ISA99 series;^[11] the Federal Energy Regulatory Commission Critical Infrastructure Protection standards, which are developed by the North American Electric Reliability Corporation;^[12] the Health Information Technology for Economic and Clinical Health Act of 2009;^[13] and the Payment Card Industry Data Security Standard.^[14]

This document is only available to subscribers. Please log in or purchase access.

[Purchase Login](#)