COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2022
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 now 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 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 cyberincidents help** in relieving the chaos that comes in the wake of a cyberattack, quickens mitigation efforts, and improves public response.
- **Cyberawareness 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 cybersecurity approach that takes both reactive and proactive strategies into account.
    - IT security can no longer be the hub of cyberdefense 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, 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 threat actors. 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 trade secrets and 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 *2019 Internet Crime Report* released in February 2020 illustrates an ongoing trend: "Internet-enabled crimes and scams show no signs of letting up…IC3 received 467,361 complaints in 2019—an average of nearly 1,300 every day—and recorded more than $3.5 billion in losses to individual and business victims".[4] The year 2020 came with its own challenges to organizations, as the coronavirus pandemic drastically altered business operations. From remote work challenges to new COVID-19–related phishing scams, cybercrime abound.

According to a 2020 report published by McAfee, the monetary loss from global cybercrime was an estimated $945 billion. The report states:

> The COVID-19 crisis has provided a fertile environment for cybercrime. Not only were criminal actors able to quickly modify their schemes in response to the pandemic, they also take advantage of the quick adoption of remote access infrastructure for work and education. Traditional schemes became 'COVID-themed.'[5]

The COVID-19 pandemic illustrates the adaptability of cybercriminals. Given society's pronounced reliance on interconnected technologies and devices to maintain business continuity in the face of the pandemic, the threat

landscape only widened and the stakes became even higher.

With these trends, it is most likely that handling a cyberevent is a matter of **when, not if**.

In spite of these statistics, the United States does not have universal federal legislation related to data security, nor a data breach reporting standard. In the absence of legislation, President Barack Obama issued an executive order in 2013,[6] outlining a framework to reduce cyber risk to critical infrastructures. The order encourages better communication between government and industry and fosters the creation of a set of standards, methodologies, procedures, and processes. The order dovetails with the dozens of industry-based or activity-based requirements that support an improved risk and compliance posture. These include, but are not limited to, the joint standard of the International Organization for Standardization and the International Electrotechnical Commission, known as ISO/IEC 27002:2013;[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]