Cybersecurity basics for in-house counsel

Help your organization manage cyber risks by bridging the understanding gap between IT and the C-suite

White paper

THOMSON REUTERS®

The FBI reported that cybercrime-related costs in the United States exceeded $4 billion in 2020 alone.[1] Some observers expect those costs to exceed $10 trillion globally in just a few years.[2]

For businesses around the world, cybercrime looms as a massive and ever-increasing threat. The FBI reported that cybercrime-related costs in the United States exceeded $4 billion in 2020 alone.[1] Some observers expect those costs to exceed $10 trillion globally in just a few years.[2] Simultaneously, legal obligations and regulators' expectations around reasonable security measures continue to expand. As in-house counsel with the right knowledge and skills, you can play an essential role in protecting your business from cyber threats and their related costs.

Despite the expanding threat of cyberattacks, many companies are poorly equipped to prevent or respond to them. For example, information technology (IT) and cybersecurity professionals have little access to C-level leadership, according to a recent study. And when they do have conversations, IT professionals may communicate in vague or poorly understood techno-jargon, frustrating executives who want clear talk and value action.[3]

This understanding gap often causes business leaders to:

- Underestimate cyber risks
- Fail to fund the proactive security controls that regulators deem necessary to meet a reasonable security measures standard

Knowledgeable in-house counsel are uniquely positioned to bridge this understanding gap. In fact, an Association of Corporate Counsel survey found that legal teams play a key role in the cybersecurity strategies of more than 70% of companies.[4] But to serve as a trusted intermediary between IT and the C-suite, you need a working knowledge of cybersecurity technology and program basics, as well as a familiarity with federal and state regulatory requirements.

When you know the basic terms and challenges, you can more accurately portray cyber risks to business leaders. As a trusted counselor and advocate for sound risk management practices, you can play a key role in developing the strong cybersecurity program and posture that your company needs.

Assessing your company's cyber risk posture

Your organization's cyber risk posture is a combination of its abilities to manage identified cybersecurity risks, respond to newly reported vulnerabilities, and defend against evolving threats. Assess your company's cyber risk posture by asking questions of key personnel and listening carefully. Their responses offer a window into what's unique about your organization's business data, infrastructure, and vulnerabilities.

You should understand your organization's IT infrastructure and processes, including any industrial control systems or other operational technology (OT), in addition to the personal information and other sensitive or confidential data that it handles. As in-house counsel, you must also recognize and offer advice on whether your organization owns or operates critical infrastructure and is thus subject to additional cyber risks and regulatory scrutiny. For example, the Department of Homeland Security (DHS) has defined 16 critical infrastructure sectors, spanning a wide range of public and privately owned assets and businesses.[5]

Conducting regular cyber risk assessments and acting on identified gaps is the foundation of any reasonable information security program. Cyber risk assessments come in different forms and are often highly technical or operational in nature.

Protect your risk assessment reports. If they fall into the wrong hands, they may become a roadmap for bad actors ready to exploit your company's cyber vulnerabilities.

In-house counsel plays an important role in these assessments by helping the business understand its potential legal liabilities and prioritizing its actions. Ask questions like:

- What are the threats to our organization's IT and OT assets, infrastructure, and data?
- What are our cyber vulnerabilities, including potential hardware, software, networking, configuration, policy, process, and human issues?
- What role do we play in various supply chains and what other organizations provide us with products and services that may contain additional vulnerabilities or offer attackers an entry vector to us?
- How likely is it that a bad actor will exploit our vulnerabilities?
- What is the degree of harm that a cyber incident might inflict on our organization?

By diving deeper into your organization's role in the broader cyber ecosystem and common cyberattack types, you can:

- Refine your risk assessments
- More clearly convey the nature and potential impact of cyber risks in language the C-suite understands
- Support a more effective risk management strategy

Proactive cyber risk management

Effective cyber risk management is a proactive, dynamic process — a continuous cycle of assessing, doing, and tracking. As a trusted counselor, your legal and risk management expertise helps your organization's IT team and business leaders to better evaluate and prioritize risk decisions and actions, and tweak the process as the threat landscape evolves.

These four common risk response strategies can help you determine what is reasonable when addressing identified gaps:

1. **Remediate:** Analyze the identified risk and devise countermeasures that effectively neutralize the vulnerability. Remediation typically closes the risk gap and is an attractive response. Patching software or updating hardware or software configurations are common ways to remediate cyber vulnerabilities.
2. **Mitigate:** Sometimes the most realistic reaction to a risk is a best-we-can-do-for-now response. That's mitigation. The organization implements policies, processes, or partial technical solutions that minimize the vulnerability and lessen the likelihood of a successful attack. Companies should periodically review their countermeasures and seek to move from mitigation to remediation when feasible.
3. **Transfer:** If the organization cannot or chooses not to remediate or mitigate a risk, it may be able to transfer it to another entity. Cyber insurance policies transfer the risk of certain costs associated with some cyberattacks to the insurer. Alternatively, the organization may outsource certain operations in a way that transfers some of the risk burden to the service provider. While these options can offer some relief, organizations typically cannot transfer their accountability and the legal liability remains.
4. **Accept:** Accepting a risk with or without further mitigating controls is a legitimate choice, especially when technical or cost barriers limit other options. However, like with mitigation, companies should periodically review their risk acceptance choices and consider whether other options have become workable.

Information sharing programs

As cyber-savvy in-house counsel, you can also help your organization effectively participate in cybersecurity information sharing programs to learn about new risks and other organizations' successful defense measures. With the appropriate safeguards, organizations can share valuable and actionable information with like-minded communities without disclosing their own vulnerabilities or other personal or sensitive information.

When planning and guiding the information sharing process:

- Consider the support of the Cybersecurity Information Sharing Act of 2015, which includes certain liability protections for private entities that monitor their IT systems or share cybersecurity information under its provisions.
- Explore the potential benefits offered by participating in DHS and industry-sponsored information sharing programs. The DHS Cybersecurity and Infrastructure Security Agency distributes general vulnerability and other cybersecurity-related information on its National Cyber Awareness System website.
- Identify other cyber information sharing organizations that are relevant to your organization's interests and review their membership agreements.
- Counsel your organization on developing and implementing policies and procedures to gain benefits from cyber information sharing while minimizing any risks.

Understanding the top cyberattack categories

Though cybersecurity threats and cyberattacks are constantly evolving, these four categories can help you organize and consider how to best defend against the most prevalent types:

1. Direct cyberattacks on users and consumers

These attacks focus on the human element of the cybersecurity equation. Common examples include tempting people to click on dangerous links or open suspicious emails or using veiled threats to prompt a desired action. These attacks also take advantage of weak user authentication practices, such as reusing passwords or failing to use multifactor authentication. Some more specific forms include:

- **Social engineering:** These attacks prey on human emotion and use psychological manipulation to entice individuals into divulging information or taking actions that allow attackers to gain access to systems or data or financially benefit, such as from misdirected money transfers. Attackers often leverage worries over real events or claim to be acting on behalf of upper management. These attacks occur in many forms and guises, including phishing, and may involve a single message or a long-term series of communications and interactions.
- **Phishing:** Phishing attempts often appear to be emails, texts, or other messages from a valid, trusted source, such as a company or individual the target knows. If the phishing attempt successfully fools the target into performing the desired action — typically, clicking a link or opening a file — attackers can collect sensitive information or install malware (malicious software) to gain access to systems or data or both. The FBI's Internet Crime Complaint Center reports that phishing attempts claimed more victims in 2020 than any other internet-based crime.[6]
- **Ransomware:** Ransomware combines a malware attack with extortion. Attackers use phishing or other means to install malware that encrypts data, or otherwise makes computer systems or data unusable, and then demand a ransom payment. These attacks also increasingly involve data theft, allowing the attacker to further threaten the victim with exposing sensitive information.

Your organization may have strong cybersecurity defenses, but one or more of your service providers may have considerably less robust practices.

Individuals and companies of all sizes can be ransomware targets. Ransom requests may range from hundreds of dollars to millions. Paying ransoms may not result in reliably regaining data or systems access, and without additional actions, an organization's systems likely remain compromised and vulnerable to further attack. Making payments to international cybercriminals can also put companies at risk of violating Office of Foreign Assets Control (OFAC) sanctions.

2. Direct cyberattacks on infrastructure

These attacks probe for and exploit vulnerabilities in an organization's IT or OT infrastructure. Attackers gain unauthorized access to networks and systems, steal sensitive data, sabotage systems, deny service to end users, or cause other issues. Common attacks include:

- **Hacking:** This is a general term for attempting to exploit cyber vulnerabilities to gain unauthorized online access to networks, systems, or data. Hackers often use information they gain through social engineering to further their attacks and may focus their intrusion attempts on potential access points such as web servers and other internet connections, remote access gateways used for telecommuting and mobile devices, wireless networks, and extranet connections that link to business partners' networks.
- **Cloud environment breaches:** Cloud-based infrastructures are also vulnerable to attack and are frequent targets, often due to poor customer configurations. A recent study found that 80% of companies suffered a breach of cloud-based data over an 18-month period in 2019 and 2020.[7] And in 2020, according to one report, in some cases, cybersecurity breaches occurred more frequently with cloud-based systems and data than with internal assets.[8]
- **Insider threats:** Insider attacks may come from disgruntled employees, especially those with privileged or other high-level access, or recently terminated employees whose access the company has failed to promptly or properly shut down. From 2018 to 2020, insider cybersecurity incidents increased by 47%, according to one study.[9]

3. Indirect cyberattacks through service providers

In this type of attack, bad actors attempt to reach their ultimate target or group of targets by exploiting a vulnerable service provider. These service providers may deliver any of a variety of IT or other services that involve their having access to customer organizations' networks, systems, or data. The widely reported 2013 Target data breach, which apparently exploited stolen service provider access credentials to the company's systems, is an example of this type of attack.[10] The Secret Service recently released an alert for customers of managed service providers, which face a rise in these attacks at least partly because of their increased popularity during the pandemic and continued IT talent shortages.[11]

Your organization may have strong cybersecurity defenses, but one or more of your service providers may have considerably less robust practices. Attackers can exploit these weaknesses and potentially access your organization's high-value systems and data.

4. Indirect cyberattacks through the supply chain

Similar to attacks on service providers, attacks through the supply chain exploit security weaknesses in a supplier's development, manufacturing, or distribution environment to reach their ultimate targets. Attackers insert malware or create cyber vulnerabilities in IT or OT software or hardware that the supplier's customers purchase or license and use. Depending on a customer's particular configuration and exposure, on installation of the supplier's products, attackers may exploit the malware or product vulnerabilities to access the target organization's systems or data or both.

A clear, well-tested cyber incident response plan provides the business with a roadmap for responding to these unfortunate but all-too-common events.

Supply chain attacks are increasing, according to the European Union Agency for Cybersecurity,[12] and they worry cybersecurity experts. A single attack on a single supplier can rapidly propagate through a large community of downstream customers. These sophisticated attacks may go undetected for a significantly long time period, compounding the damage.

Real-world examples of reported supply chain attacks include: [13]

- In 2020, purportedly nation-state sponsored hackers compromised Texas-based SolarWinds' systems and added malicious code into the company's IT network management software. The code created a backdoor to certain exposed customers' systems that hackers then used to further target private and public sector victims.
- In 2016, a U.S. cell phone manufacturer used software from a foreign company in its devices. Apparently unknown to the manufacturer, the software regularly transmitted text, call details, and contact information to non-U.S. servers.
- A U.S. software company discovered malware preinstalled on one of every five tested laptop and desktop computers. The malware was apparently installed downstream from the point of manufacture.

Steps to protect your organization

As knowledgeable in-house counsel, you can help protect your organization from these types of cyberattacks and their unfortunate consequences by:

1. Identifying your organization's legal obligations to protect the data and systems that cyberattacks may compromise
2. Consulting with your IT team and business leaders to evaluate the degree of risk that your organization's IT and OT infrastructure faces and close identified gaps, according to risk and exposure levels (see Assessing your company's cyber risk posture)
3. Taking a comprehensive approach to information security by developing, implementing, and maintaining a written information security program (WISP)
4. Making thorough due diligence and ongoing oversight part of the vetting process for potential and current service providers and suppliers, including performing a careful review of their testing protocols and certification processes for hardware and software
5. Advocating for a strong employee cybersecurity training program along with reasonable technical controls, monitoring, and a robust cyber incident response plan

You can also leverage your position as a trusted advisor to increase senior management's engagement with and support for cybersecurity programs to help reduce risks

Cyber incident planning and response

A clear, well-tested cyber incident response plan provides the business with a roadmap for responding to these unfortunate but all-too-common events. Counsel's role in creating this plan includes helping select the incident response team, identifying and helping business leaders manage liability risks, ensuring smooth communications, and more. Considering whether, when, and how to notify law enforcement of a cyber incident, often with outside counsel support, is a key component of any cyber incident response plan.

The importance of building relationships with law enforcement agencies

You and your organization must respond rapidly when experiencing a cyber incident. You may choose to contact relevant federal, state, or local law enforcement agencies, according to the specific facts and circumstances. In-house counsel can streamline your organization's incident response by establishing relationships with these agencies before an incident occurs and maintaining a list of those contacts.

Consider making contacts with relevant federal agencies, which may include:

- The DHS CISA
- The Federal Bureau of Investigation
- The Secret Service
- U.S. Immigration and Customs Enforcement
- The U.S. Postal Inspection Service
- The Bureau of Alcohol, Tobacco, Firearms, and Explosives

Providing counsel on today's most important issue

As in-house counsel, you're expected to maintain a working-level expertise about a range of different issues. In today's corporate world, there's nothing more pressing than cybersecurity. A recent International Bar Association article reported that companies are increasingly turning to in-house counsel for cybersecurity guidance.[14] The clear takeaway is that cybersecurity is not the sole responsibility of the IT team.

To provide effective guidance in your ever-expanding role, you need a foundational level of knowledge about the most common cyber risks, attack vectors, and information security program elements. You don't need to become a techno-geek or even a cyber expert. However, you must possess enough knowledge to:

- Understand applicable laws and regulations
- Bridge the understanding gap between IT and business leaders
- Ensure that the organization effectively manages its cyber risks and maintains reasonable security measures

These are natural extensions of your role as trusted counselor and protector of the business

No matter how sophisticated or nascent your cyber knowledge or your business's cybersecurity program is, Thomson Reuters® Practical Law gives in-house counsel the trusted information and resources needed to protect the business against current and growing cyber threats.

Start your free trial today!

About the author: Melodi (Mel) Gates

Melodi (Mel) Gates, CIPP/US joined Thomson Reuters from Squire Patton Boggs (US) LLP, where she focused on cybersecurity and privacy issues. Prior to practicing law, Mel spent 20+ years in the telecom industry, last serving as CISO for a large network provider.

[1] Federal Bureau of Investigation, "2020 Internet Crime Report," March 17, 2021, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[2] Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybercrime Magazine, April 27, 2021, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[3] McKinsey & Company, "Perspectives on transforming cybersecurity," March 2019, https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

[4] Association of Corporate Counsel, "ACC Foundation Cybersecurity Report: Majority of CLOs Lead Their Organization's Cybersecurity Efforts, July 28, 2020, https://www.acc.com/about/newsroom/press-releases/acc-foundation-cybersecurity-report-majority-clos-lead-their.

[5] Cybersecurity & Infrastructure Security Agency, "Critical Infrastructure Sectors," https://www.cisa.gov/critical-infrastructure-sectors.

[6] Federal Bureau of Investigation, "2020 Internet Crime Report."

[7] "Nearly 80% of Companies Experienced a Cloud Data Breach in Past 18 Months," Security Magazine, June 5, 2020, https://www.securitymagazine.com/articles/92533-nearly-80-of-companies-experienced-a-cloud-data-breach-in-past-18-months.

[8] Maria Korolov, "Report: Cloud Security Breaches Surpass On-Prem Ones for the First Time," Data Center Knowledge, May 20, 2020, https://www.datacenterknowledge.com/security/report-cloud-security-breaches-surpass-prem-ones-first-time.

[9] Proofpoint, "2020 Cost of Insider Threats: Global Report," July 7, 2021, https://www.proofpoint.com/us/resources/threat-reports/2020-cost-of-insider-threats.

[10] Miloslava Plachkinova and Chris Maurer, "Teaching Case: Security Breach at Target," Journal of Information Systems Education, Winter 2018, https://jise.org/Volume29/n1/JISEv29n1p11.pdf.

[11] United States Secret Service, "Compromised Managed Service Providers," June 12, 2020 https://s3.documentcloud.org/documents/6980788/US-Secret-Service-PIN-on-MSP-attacks.pdf.

[12] Homeland Security Today, "Supply Chain Cyber Attacks Expected to Quadruple, Says EU Agency," August 2, 2021, https://www.hstoday.us/subject-matter-areas/cybersecurity/supply-chain-cyber-attacks-expected-to-quadruple-says-eu-agency/.

[13] Cybersecurity and Infrastructure Security Agency, "Defending Against Software Supply Chain Attacks," April 2021, https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf.

[14] Lucy Trevelyan, "Companies turn to in-house teams for cybersecurity," July 1, 2021, International Bar Association, https://www.ibanet.org/companies-turn-to-in-house-teams-for-cybersecurity.

© 2021 Thomson Reuters TR2015681 11/21