ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Advanced Persistent Threats: Effective Response to Nation-State Attacks

Technology, Privacy, and eCommerce

Corporate, Securities, and Governance


Critical Security Update
Install Now


Critical Security Update
Install Now

CHEAT SHEET

- ***An APTitude for sowing disaster.*** Advanced Persistent Threats are organizations funded or supported by state actors that target a corporation's data for some strategic objective.
- ***Accept your limitations.*** Sophisticated hackers can infiltrate virtually any company, given enough time and resources.
- ***Don't mistake compliance for security.*** Real security goes beyond compliance — today's regulation does not sufficiently mandate preparedness for data threats.
- ***Culture beats tech.*** Technical solutions will only take you so far; inculcating a culture of preparedness is also required to lower your risk of a breach.

> "Cybersecurity is now a persistent business risk … The impact has extended to the C-suite and boardroom."
>
> – 2015 PwC "Global State of Information Security Survey" of over 9,700 senior global executives

Are you ready to offer the right advice to help your company prepare for an attack by foreign agents intent on stealing your company's trade secrets and intellectual property? How would you respond if a foreign government group targets your executives for public embarrassment and destroys content (known as a "wipe and release" attack), as happened last year to Sony? These examples are not one-time attacks perpetrated solely for quick money. These are attacks by an advanced persistent threat (APT), a well-resourced actor (commonly) with some degree of nation-state sponsorship. While an APT will exploit a system using the easiest and least costly mechanism, APTs also have the ability to exploit unknown security vulnerabilities (known as a zero-day exploit) and other sophisticated tools and tactics to destroy brand reputations, suck out confidential trade secrets and steal millions of dollars or euros annually.

APT threats are capable of doing substantial damage. The cost of APTs has demonstrated the seriousness of the threat. As an example, after the Target Corporation suffered an APT attack:

- Profits fell 46 percent in Q4 2013.
- Target reportedly spent US$ 61 million (€55 million) mitigating the breach.
- The company is facing more than 100 lawsuits and some analysts forecast breach-related losses could top $1 billion (€91 million).

In many companies, chief legal officers (CLOs) now supervise chief information security officers (CISOs) and compliance officers. This requires the CLO to adequately understand the company's approach to preparing for, and responding to, serious threats like APTs. The solution is not solely a technical challenge. The CLO must play a critical role in setting the policy foundation for a security program. They must also effectively communicate the threat to the board of directors, coordinate executive team communication and be prepared to suggest an effective risk management strategy.

This article will help you understand today's most serious cybersecurity threat — the APT. This article

also covers some of the key concepts you should understand about advanced cybersecurity threats and how you can properly prepare for these threats as a CLO.

What is an APT and why is it the most dangerous cyber threat?

An advanced persistent threat, or *APT*, is the security industry term for groups that typically have some degree of nation-state sponsorship. These groups launch coordinated persistent attacks to penetrate a company's defenses, sometimes in response to nation-state direction or in support of national objectives. APTs generally do not launch single incident attacks. They generally, and persistently, establish a foothold inside the company for the purposes of reconnaissance, exploitation, data theft, data alteration, data destruction and ongoing surveillance. These attackers are classified as "advanced" because they are typically government agents with teams of hackers, often with unique skill capabilities, and the support of large government resources. They are termed "persistent" because they attack relentlessly with the aim to penetrate the target and stay as long as possible on a system. In a 2014 study of advanced threat persistence, the average advanced attacker stayed inside a company's system for 205 days — with one threat group hiding for over eight years inside a company's network!

Social engineering: Why your executives WILL download malware

APTs don't always use advanced techniques and still rely heavily on social engineering to expose secrets or access systems. Almost 80 percent of phishing emails sent to company executives in 2014 were disguised as emails from the corporate IT security group requesting the executive to provide an access password.

The use of sophisticated and personally tailored emails sent by APTs to victims is referred to as spear-phishing. Recent examples have included emails sent to senior executives that appear to be from trusted sources and include unique industry terms or previously stolen private data that easily deceives a target into believing the message is legitimate.

One example is an APT group that currently targets medical and pharmaceutical executives with sophisticated spear-phishing emails. This group is believed to be stealing information about new biotech discoveries in an attempt to use this private information for stock trading. This APT group knows its audience. Their spear-phishing themes appear to be written by native English speakers familiar with both investment terminology and the inner workings of public companies. The group's spear-phishing emails frequently focus on shareholder and public disclosure concerns. The example below illustrates one spear-phishing *lure* sent by an APT group designed to have the victim click a link that would download malware:

> Subject: employee making negative comments about you and the company
>
> From: Name
>
> I noticed that a user named FinanceBull82 (claiming to be an employee) in an investment discussion forum posted some negative comments about the company in general (executive compensation mainly) and you in specific (overpaid and incompetent). He gave detailed instances of his disagreements, and in doing so, may have unwittingly divulged confidential company information regarding pending transactions.

> I am a longtime client and I do not think that this will bode well for future business. The post generated quite a few replies, most of them agreeing with the negative statements. While I understand that the employee has the right to his opinion, perhaps he should have vented his frustrations through the appropriate channels before making his post.
>
> The link to the post is located here (it is the second one in the thread): http://forum./redirect.phpurl=http://%2fforum%2fequities%2f375823902%2farticle.php\par
>
> Could you please talk to him?
>
> Thank you for the assistance,
> Name

These examples demonstrate the sophistication of APT spear-phishing attacks and the likelihood that they will be successful in gaining access to your company networks. Rather than focusing solely on prevention, it then becomes necessary to shift your focus to fast detection and response.

Why did old security approaches fail?

Traditional IT security commonly uses defined criteria or patterns to detect threats. This is similar to digital fingerprints that identify threats based on known characteristics that have been seen in a prior attacks. However, this approach was fatally flawed. APT attackers can easily make changes to malware that alters the *digital fingerprint*. Some organizations see hundreds, even thousands, of unique variabilities in malware designed to evade any pattern based detection system. This has required a new approach focused on detecting APT based on behavior and not on patterns or *signatures*.

An even more serious, and advanced, attack is the use of a *zero day exploit*. A zero day exploit is the security industry term for an unknown vulnerability in software or an IT system. These are unknown doors into systems that can be incredibly valuable for attackers to exploit. They are very difficult to detect and can cause large amounts of damage. APT may use a zero day exploit to launch a *zero day attack* that exploits this unknown vulnerability to enter and harm an organization.

The seriousness of zero day attacks was highlighted recently in a 2014 study by KPMG of 20 large European multinational companies that found that 93 percent of the organizations were breached, with 79 percent of the attackers stealing confidential data. Fifty percent of these attacks were successful by exploiting previously unknown, zero day exploit vulnerabilities. By creating a unique zero day attack, an APT group can bypass any security that is based on defined patterns or “digital fingerprints.” This makes the detection and elimination of zero day vulnerabilities a primary concern for IT security managers trying to shut the door on APT.

Your IT security team is going to lose some battles: Be prepared

In 2014, Bank of America CEO Brian Moynihan stated that he was giving his IT security team a financial blank check to implement security, but even with unlimited resources, the CEO noted that “it is going to be a continual and likely never-ending battle to stay ahead of it [cyber threats] — and, unfortunately, *not every battle will be won.*” Even with unlimited resources, you are still more likely than not to be breached.

The recent attack against Sony by North Korea is only the most recent and highly publicized, but there have been thousands of attacks conducted globally by APTs. One of the earliest known large scale APT attacks was the Aurora attacks in 2010 in which Google disclosed it was one of more than 20 companies successfully targeted by a coordinated effort to gain access to sensitive systems and confidential information. Known targets of the Aurora group spanned a variety of industries, including the financial, technology and chemical sectors. The Aurora attackers, believed to be agents of a large Asian government, used a zero day attack to enter company targets with the aim of locating and extracting confidential trade secrets. These trade secrets could then be transferred to commercial competitors in the attacker's country and destroy the competitive advantage of the victim company.

Knowing your company has a high chance of being attacked by an APT, there are three foundational truths you must accept as a general counsel:

1. An ATP breach is probably inevitable.
2. There is no "silver bullet" technical solution to prevent a breach.
3. The solution is to focus on preparation, fast detection and fast response.

What can you do to prepare?

> "Corporate boards need to ensure that management is fully engaged in developing defense and response plans as sophisticated as the attack methods, or otherwise put their company's core assets at considerable risk."
>
> — National Association of Corporate Directors (NACD), Director's Handbook Series, Cyber-Risk Oversight.

Ninety percent of directors participating in the NACD governance survey indicated they would like to improve their understanding of cybersecurity risk, but they need executive leadership in the company to help them. As the NACD study further emphasized: "It is incumbent upon the executive team to take ownership of cyber risk and ensure that the board understands how the organization will defend against and respond to cyber risks." Over half of boards are still not involved in security strategy and 75 percent are not reviewing security and privacy risks. This needs to change if you want to be prepared to respond to an APT attack.

An ethical and effective response

The security community is currently struggling with serious ethical questions related to what extent offensive technical capabilities or potentially intrusive monitoring may be appropriate as part of an effective security program or incident response program. This topic ranges from use of "cyber weapons" against adversaries to aggressive gathering of threat intelligence that may violate personal privacy. These are issues that require very careful consideration by the CLO and chief ethics officer. Many global laws restrict the degree of monitoring or types of response that is allowable. In the United States, the Computer Fraud & Abuse Act (CFAA) sets criminal penalties for unauthorized hacking — even if the activity is a "hack-back" in response to an attack. The European Union also has very strict laws protecting personal privacy in the workplace. Your company will need to consider, ethically and legally, what security activity will be appropriately tolerated to be secure.

Cybersecurity ethics is a complex topic that requires a lengthy analysis. However, for the purposes of this article, you should be aware that you should include consultation by your chief ethics officer and

careful consideration of the ethical limits that are appropriate for a security program. Be aware of the need to restrain the sometimes natural impulses of executives to “punch back” when attacked. This may not only be ineffective, but also unethical and possibly illegal. There may better options, such as legal “takedowns” of attacker infrastructure that the CLO may help to pursue. Some companies have successfully used legal seizure laws or cooperated with law enforcement to respond to cyber-attacks. These methods may be more effective and not risk the legal or ethical issues created by technical counter-attacks. Whatever response solution is chosen, it should be validated as legal and ethical. This is a critical part of overall incident response planning.

How “good” do you need to make security?

You need to understand your company, your market position and what’s at stake to understand how “good” you need to be — and you DO need to decide. This is a tough question to answer but it will determine your corporate security strategy. Don’t leave this critical decision solely to the CISO. Demand assurance that your security team understands the most important company information. Ensure they are taking adequate steps not just to be compliant with regulations but really address the more advanced security threats like hunting for APTs on your network. If a foreign competitor steals your trade secrets, your entire IP protection program may be a waste of time. Make sure your company is taking both the legal and technical steps to protect its intellectual property.

Even if your company is “only baking cupcakes,” you should still be concerned about APT because of their propensity to move “upstream.” The most recent example of this is the recent massive Target store data breach. In this example it is believed that the attack began through an HVAC supplier connected to the Target network. The APT used this HVAC supplier to access a much larger victim — Target. The recent Sony attack also revealed that even the entertainment industry could be a target of an APT nation-state attack.

Talking to your board about security

The APT threat has become a board issue. As the executive in charge of risk management, if you do not drive a board discussion on this topic yourself, you have to at least be prepared for a meeting with the board of directors about APT and know what questions they will ask. Some questions you should expect include:

- What’s going on out there?
- Who is after us?
- Are we being targeted?
- How and where are they aiming?
- What are they after?
- Have we already been compromised?
- Are we prepared to sustain an attack?
- How fast can we detect, respond and recover?
- Can we prevent bad things from happening?
- Where should we focus (and not focus)?
- How much is enough?
- How can I not impede my business productivity?
- How do I continue to *manage* these risks?

Coordinate with your internal security team leader (chief information security officer) to establish your

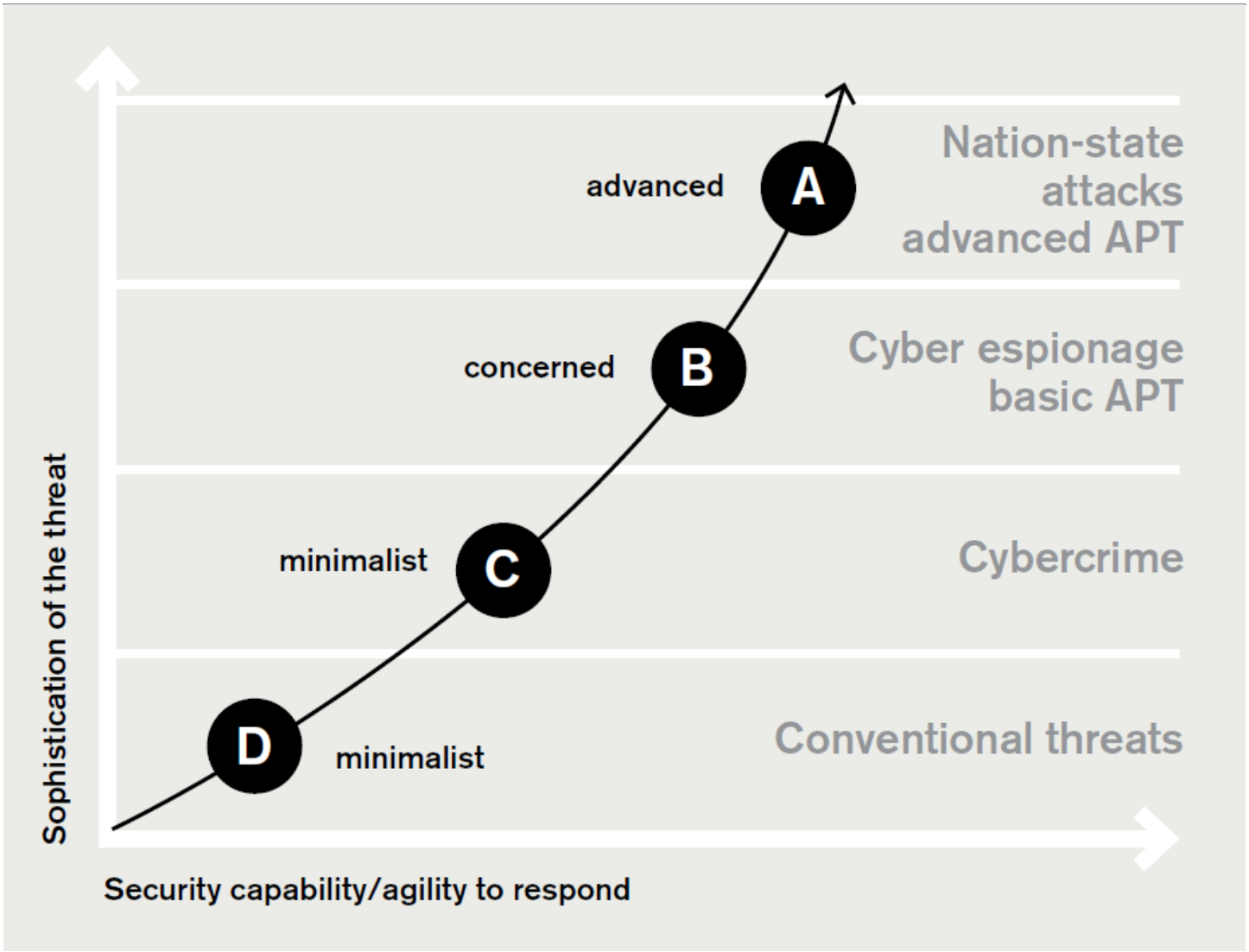
company’s correct position on a scale of a capability maturity model. Not every company needs the most advanced security, but answering “How good do you need to be?” and what type of cyber insurance risk management program you need should be part of a collaborative discussion with the CISO and CLO. This includes knowing what types of company data might be valuable to an attacker, the type of confidential information your company maintains, where it is stored and what is most sensitive. Although the security team might conduct much of this work, the CLO can provide valuable insights on this information and probably already tracks the most important information for other legal purposes.

Capability maturity model

Once you decide “how good you need to be,” you should adopt a policy based risk management approach:

Oversight of the technical security process may be led by the CISO, but the CLO can drive a cross team collaborative approach. Security is a process. It requires a governance structure to serve as the support mechanism to steer the program and resolve critical decisions. Having cross-functional support greatly helps in justifying policy change, budget and the company cultural change you may require to be successful. This is the structure you need to make your strategy a living strategy and maintain business awareness when a breach occurs.

Capability maturity model



An Executive Security Steering Committee (ESSC) should meet quarterly and a Security Technology Architecture and Risk Committee (STARC) subcommittee should meet monthly. Some CISOs are only technical focused and may not understand all of the legal issues related to compliance. Similarly, legal staff may not fully understand technical issues caused by policy decisions. Collaboration is essential for success. This structure of an ESSC and a STARC subcommittee create an ongoing internal framework for strong security preparedness and response.

Without a solid internal structure, you will have trouble building any success. Smart risk management policy and internal coordination are the foundation preparing for advanced threats and managing your security program.

How can effective risk management save your company money?

How to lower your insurance premiums

The basic premise of risk management is saving money and shifting risk appropriately. The better you can demonstrate your company's security posture and resiliency to the insurance market, the better the outcome for your company — fair premiums, higher limits, fewer claims — a win for everyone

involved.

The insurance industry typically uses a *prevention and claims* approach, where it's believed the more money you put into preventative activities the less likely claims are to occur. But because 100 percent prevention of APT threats is not a feasible goal, you should consider advocating a *monitor and respond* approach to lower premiums. Underwriters should understand your internal security team's technical ability to prevent attacks from occurring, but also, as legal counsel, you can take it a step further to demonstrate your ability to respond to exposures to minimize losses after they have occurred. This is the story that you need to be armed with in order to best present your enterprise to the insurance market and achieve the desired goal of lowering premium costs. Outline your internal structure of an executive security committee and your ability to use a cross-functional security management process to respond to attacks. Keep in mind that underwriters will look at a number of factors to arrive at their premium, but all other things being equal, advocating this approach provides a clear risk differentiator that should have underwriters competing for your business.

Limit liability with the US Safety Act

The SAFETY Act is a 2002 US law that created a liability management program for providers of antiterrorism technologies and it can be directly applied to help protect your company against liability arising from ATP attacks. The SAFETY Act creates liability limitations for "claims arising out of, relating to, or resulting from an Act of Terrorism" where antiterrorism products have been deployed. Under the SAFETY Act, certain security product and service providers may apply for liability protections — in the form of a SAFETY Act award — from the US Department of Homeland Security (DHS). If awarded SAFETY Act protections, the provider is entitled to specific protections from third party liability stemming from the use of that product or service in relation to an "Act of Terrorism" *and liability protections associated with this award "flow down" to the buyers of these technologies.*

Support Anti-terrorism by Fostering Effective Technologies Act of 2002, 6 C.F.R. Part 25. 2 71 Fed. Reg. 33, 147, 33, 156 (June 8, 2006, Final Rule).

The DHS Secretary has to declare that the cyber-attack in question is an "Act of Terrorism." However, under the law, "Act of Terrorism" is broadly defined. The attack only needs to be 1) unlawful, 2) cause harm, including economic harm in the United States, and 3) the attacker has to use a weapon or other items that are intended to cause such harm. There is no need to demonstrate "terrorist" motivations or connections to terrorist groups. As such, the SAFETY Act can apply to a broad range of attacks, including state-sponsored or criminal cyber-attacks.

Tort claims filed against a SAFETY Act certified product user relating to the use, performance, design etc. of the certified security product, the certification provides a strong defense up to and potentially including dismissal of claims. The Safety Act also provides exclusive federal jurisdiction and a rebuttable presumption of immediate dismissal of all third-party claims based on the alleged failure of the product/service used by your company that arise out of or relate to the cyber-attack in question. The SAFETY Act can apply even when an attack originates from or actually occurs outside the United States. So long as the attack impacts the United States (either physically or economically) and the ensuing litigation is being decided under US law, both US and international companies may take advantage of the defenses of the SAFETY Act.

SAFETY Act only provides for dismissal of third party claims — regulatory and other types of claims can still proceed. The certified product must also be in the same working form and use as it was certified.

Reviewing the security products used by your company, and ensuring that they are always SAFETY Act certified, can provide very strong protection against claims arising from an APT attack.

Security risk management

POLICY

- Security policy development
- Customer and internal auditing
- Security awareness
- Compliance management
- Security process development

RISK MANAGEMENT

- Risk assessment and analysis
- Vendor management and review
- Product release assessments
- IT system security assessments
- Remediation prioritization
- Security planning and strategy
- Security governance
- Business continuity

What are the public policy trends related to APT?

Basic compliance is not good security. Your company goal should be real security and not merely compliance. However, as a CLO, it is important to know the global policy trends now recognizing the APT threat.

In Europe, the Network Information Security (NIS) Directive is expected to be finalized by the end of 2015 and will impose new strong security standards for many companies across Europe. Most importantly, this will likely require a large group of companies to adopt “state of the art security” controls to manage risk. As APT threats are becoming more pervasive, APT detection protocols are likely to be recognized as part of “state of the art security” requirements. The potential fines for failure to implement these controls can be significant.

Germany recently became the first EU country to adopt an updated IT security law that requires a wide range of companies to adopt “state of the art security.” The German law mandates *state of the art* organizational and technical security measures to avoid interferences of availability, integrity, authenticity and confidentiality of information technology systems. The law includes mandatory data breach reporting and regular audit requirements.

The United States government has also recognized that it is critical to adopt measures that will defend against advanced cyber threats like APT. One example of a best practice to detect APT is included in the United States NIST Special Publication 800.53 (Rev.4) and has now received widespread adoption by Fortune 500 companies. This recommendation states that organizations should implement “non-signature-based malicious code detection mechanisms” specifically designed to find zero day vulnerabilities and detect APT.

Outside Europe and the United States, governments are also adopting policy to protect against APT. In the Asia Pacific Region, the Australian Signals Directorate (ASD) in 2014 added detection of zero day APT vulnerabilities to its Top 10 of “35 Critical Strategies for Cybersecurity.” The ASD recommends that organizations implement “automated dynamic analysis of email and web content run in a sandbox to detect suspicious behavior including network traffic, new or modified files, or other configuration changes.”

While these are technical standards, it is important for the CLO to be aware of these emerging recognized best practices. They are becoming security standards and may affect your duty of care. This also provides guidance for your discussion with your security leaders about whether they are following best practices to protect your company.

The road to success

> “Accelerating investments is not enough … you have to mature your organization, your people, and your technologies, and that can be a more restraining factor than the availability of capital.”
>
> Gary Hayes, CIO of CenterPoint Energy - PWC Global State of Information Security 2014

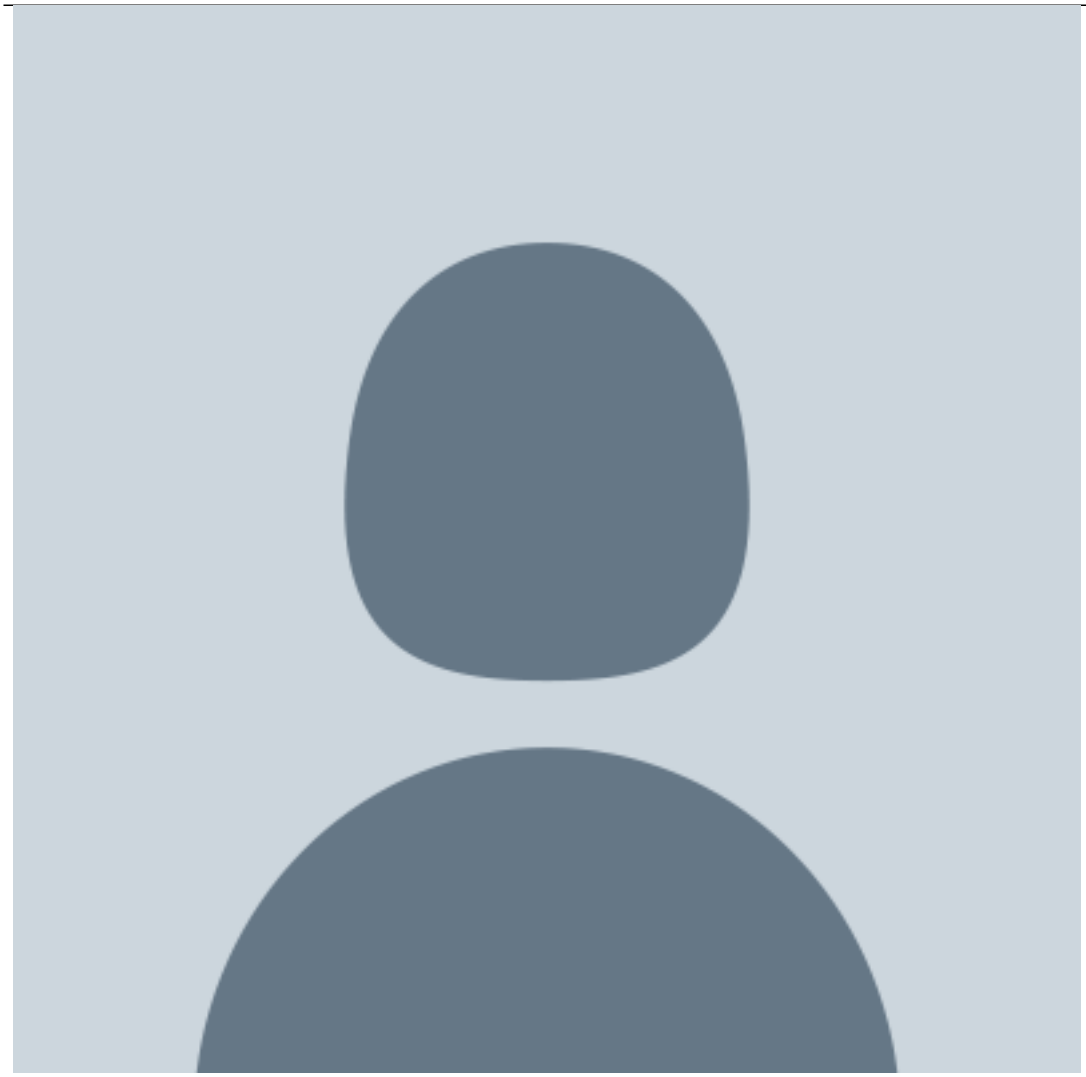
Whether you directly manage the CISO or work collaboratively as a peer with your security team leader, you play a critical role in your company’s security program. The risk of an APT attack with the ability to destroy your company’s reputation or competitive advantage is a critical concern for your

company’s health. You must be prepared to effectively communicate this message to your executive team and board.

Verify that your security team is considering not just technical solutions, but the advantages of US SAFETY Act certified solutions to detect zero day threats as these can significantly lower your liability exposure. Stay informed about the latest standard of care requirements for state of the art security now included in many government IT laws. Finally, adopting a *detect and respond* posture (anticipating a breach) vs. a prevention posture (that is likely to fail) is a strong, smart, risk management model.

Technical solutions are only part of the answer. As a CLO you can promote the correct internal risk management structure. You should take responsibility to manage preparedness, reduce insurance costs and coordinate the internal risk management structures. Your IT team may be only considering the technical solutions. However, by being actively engaged in security preparedness, you can also significantly lower the risk that an APT threat will cause significant harm.

Adam Palmer



FireEye

Adam Palmer manages all international government affairs at FireEye, an advanced cybersecurity company. Palmer is based in Munich, Germany, where he manages a global team.