It’s critical that we step back and assess the significance of these attacks in their full context. This is not ‘espionage as usual,’ even in the digital age. Instead, it represents an act of recklessness that created a serious technological vulnerability for the United States and the world. In effect, this is not just an attack on specific targets, but on the trust and reliability of the world’s critical infrastructure in order to advance one nation’s intelligence agency. While the most recent attack appears to reflect a particular focus on the United States and many other democracies, it also provides a powerful reminder that people in virtually every country are at risk and need protection irrespective of the governments they live under.

— Brad Smith, president, Microsoft (in response to the FireEye hack)
Misinformation Moats

Mid-future optimistic scenario

Pervasive hacking and threats of cyber warfare inspire a new wave of cybersecurity solutions. Borrowing from tactics used in national elections, cybersecurity companies design strategic layers of misinformation to protect their clients’ intellectual property. These moats lie just inside firewalls and act as a second barrier against hackers. Misinformation moats are filled with bad data, misleading information, and even malicious software. When hackers access the moat, they think they’ve found what they’re looking for, leaving the true payload protected.
Access control
A selective restriction that controls what data users and user groups can access, see, share, and edit.

Adware
Software that automatically generates online ads; it can also include spyware that tracks your browsing habits. It’s because of adware that many people are turning to ad blocking software.

Air gap
A system that is physically separated and isolated from all other computers, networks, and the internet.

Anonymous
A collective of hackers, best known for its use of the Guy Fawkes mask and distributed denial-of-service (DDoS) attacks. Anonymous typically uses the hashtag #Ops when announcing a new campaign. Past ops included a take-down of the Church of Scientology and the Westboro Baptist Church.

Authentication
A verification process that confirms the identity of a user based on specific information.

Backdoor
Developers intentionally install backdoors into firmware so that manufacturers can safely upgrade our devices and operating systems. The challenge is that backdoors can also be used surreptitiously to access everything from our webcams to our personal data.

Black hat
A malicious hacker; someone who hacks for personal gain.

Bot
Bots are automated programs that perform a simple task. Some—simple chatbots, for example—are completely harmless. Other bots can be programmed to repeatedly guess passwords so that a hacker can break into a website.

Botnet
A botnet is a group of computers that are being controlled by a third party, and are being used for any number of nefarious purposes. For example, malware installed on your computer can run undetected in the background while hackers use your machine as part of a large spamming network.

Breach
The moment a hacker gains access to a device or network via a vulnerability.

Bring Your Own Device (BYOD)
A policy that authorizes employees to use their own devices on the company network or to access company data.

Browser hijacking
This attack changes a user’s default homepage and search engine without permission, often in order to gain clicks to websites for ad revenue or to inflate a page’s ranking.

Brute force attack
This type of attack is a laborious, methodical process where a hacker uses software to automatically guess every password it can to gain unauthorized entry into a network or computer.

Bug
A flaw or problem in a program that can be harmless or might allow hackers to exploit a system.

Cloud
Data storage or computing services that are accessed using remote servers.

Cookie
A small file sent from your computer’s web browser to a server. Cookies help websites recognize you when you return, and they also help third parties track their audience.

Cracking
A basic term that describes breaking into a security system. Anyone “cracking” a system is doing so maliciously.

Crypto
Cryptography (or “crypto”) is the art and science of encrypting data—as well as breaking encryption. (The term is also used as shorthand for the cryptocurrency market and its various tokens.)

CxO spoofing
Cybercriminals digitally impersonate a company’s executive leadership team to gain access to IP, data, or other sensitive information.

Cyberattack
An attempt by a bad actor to gain access to a computer system, device, or network for the purpose of collecting data, monitoring activity, or causing damage.

Dark web
Encrypted networks that are not easily accessible by outsiders. Users are anonymized. Illegal activities are often carried out on the dark web, such as selling company data.
## Cybersecurity Terms Every Executive Should Know

| **Data leakage** | The unauthorized access of information resulting in leaks, theft, or loss.
| **Denial-of-service attack (DoS)** | This is when a hacker sends so many requests to a website or network that the traffic temporarily overwhelms the servers, and the site or network goes down.
| **Digital certificate** | These authenticate and approve the identity of a person, organization, or service.
| **Distributed denial-of-service attack (DDoS)** | This is a DoS using a battalion of machines.
| **DNS hijacking** | This attack changes a computer’s settings to ignore a domain name system (DNS) or to use a DNS that’s controlled by malicious agents.
| **Doxing** | When hackers root out and publish personally identifying information about someone online.
| **Dump** | The term for a trove of data released by hackers.
| **Dumpster diving** | Hackers search through garbage looking for information that will help with an exploit. Organizations and individuals who don’t consistently use a shredder are particularly vulnerable to this method.
| **Encryption** | Using special code or software to scramble data so that it cannot be read by a third party, even if it is intercepted.
| **End-to-end encryption** | When an encrypted message is scrambled on both ends, as it is sent and again as it is received.
| **Exploit** | The general term for leveraging a vulnerability in a piece of code, software, hardware, or a computer network.
| **Firewall** | A system of software and hardware that’s designed to prevent unauthorized access to a computer or computer network.
| **Hacker** | This term means different things to different people. People who tinker with code, to purposely manipulate it, are hackers. Some are good, and some are bad. In popular culture, “hacker” has taken on an reductive, distinctly negative connotation.
| **Honeypot** | Someone who hacks for social or political reasons.
| **InfoSec** | An abbreviation for “information security,” InfoSec can refer to the companies and professionals who work within cybersecurity.
| **Jailbreak** | A way of removing the restrictive manufacturer’s code from a device so that you can reprogram it to function as you desire.
| **Keys** | The code that, just like a physical key, is used to lock or unlock a system, encrypted message, or software.
| **Malware** | Any software program that’s designed to manipulate a system, by stealing information, augmenting code, or installing a rogue program. Rootkits, keyloggers, spyware, and everyday viruses are examples of malware.
| **Man-in-the-middle (MitM) attacks** | This occurs when a hacker impersonates a trusted connection in order to steal data or information or to alter communications between two or more people. These are especially common in businesses.
| **Metadata** | This is the data that explains what’s in another set of data, such as a JPEG photo, email, or webpage.
| **Password managers** | These third-party tools let you remember one master password to unlock a database of all your other passwords. You can still use a completely different password for every site and service you use. While password managers are a good idea in theory, many are cloud-based. If a hacker gains access to your password manager, you’re in big trouble. So, if you do use one, make sure to use a complicated password at least 36 characters long with lots of special characters, numbers, and capital letters.
<table>
<thead>
<tr>
<th><strong>Cybersecurity Terms Every Executive Should Know</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Patch</strong></td>
</tr>
<tr>
<td><strong>Penetration testing</strong></td>
</tr>
<tr>
<td><strong>PGP (Pretty Good Privacy)</strong></td>
</tr>
<tr>
<td><strong>Phishing</strong></td>
</tr>
<tr>
<td><strong>Plaintext</strong></td>
</tr>
<tr>
<td><strong>Ransomware</strong></td>
</tr>
<tr>
<td><strong>RAT (Remote Access Tool)</strong></td>
</tr>
<tr>
<td><strong>Root</strong></td>
</tr>
<tr>
<td><strong>Rootkit</strong></td>
</tr>
<tr>
<td><strong>Screen Scraper</strong></td>
</tr>
<tr>
<td><strong>Social Engineering</strong></td>
</tr>
<tr>
<td><strong>Spearphishing</strong></td>
</tr>
<tr>
<td><strong>Spoofing</strong></td>
</tr>
<tr>
<td><strong>Verification</strong></td>
</tr>
<tr>
<td><strong>Virtual private networks (VPNs)</strong></td>
</tr>
<tr>
<td><strong>Virus</strong></td>
</tr>
<tr>
<td><strong>Vulnerability</strong></td>
</tr>
<tr>
<td><strong>White hat</strong></td>
</tr>
<tr>
<td><strong>Worm</strong></td>
</tr>
<tr>
<td><strong>Zero-day exploits</strong></td>
</tr>
<tr>
<td><strong>Zombie</strong></td>
</tr>
</tbody>
</table>
Those who work in innovation have a unique set of skills that could aid in a company’s approach to privacy and security. One of the biggest challenges faced by companies is that they do not think creatively about adversaries or next-order outcomes. For example, before a company launches a new product, it would be useful to host a workshop to deeply investigate all of the possible ways the product could unintentionally cause harm—or bring harm to the business.

Privacy and security should be top of mind among R&D teams, but within many companies, R&D units struggle to keep pace with the changing technology landscape. This results in pet projects taking up too much time, even when they don’t lead to desired results—or moving too quickly on projects without considering their security or privacy implications. The cadence of R&D teams must be adjusted to accommodate emerging privacy and security considerations.

Cyber espionage is a growing threat, and successful companies are clear targets: Criminals want to steal valuable IP from the world’s best businesses. Chief risk management officers and those who work in risk-related positions can play a critical role in protecting a company’s most important assets by championing data auditing, promoting proper data governance and management, and advocating for a risk-driven approach in departments that rely on data.
We recommend using this report to support your strategic foresight activity in the coming year. Every executive team should begin by asking these questions about security and privacy:

1. Is our company’s board of directors briefed regularly by our CISO?
   Is our board fully engaged in issues related to privacy and cybersecurity?

2. What parts of our business make us a target for attacks?
   When was the last time we audited the systems that keep those parts of our business safe?

3. Will our current approach to data collection, storage, encryption (and, if applicable, reselling) cause future problems?
   What assumptions must hold true for our current strategy to succeed?
   How will we make needed changes?
Selected Sources

https://world-at-home.tanium.com/
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
https://googleprojectzero.blogspot.com/