Cybersecurity Commands More Attention as Threats Mount

August 2020

Adam Shane, PSP MSEE
Systems Integration Manager

Cybersecurity may be the most widely recognized word in the English language, but few people fully understand its meaning. Cybersecurity is a set of practices that are focused on limiting the impact of hackers on corporate cyber assets (networks, servers, workstations, mobile devices, and data).

Cybersecurity is growing in corporate awareness. In 2004, worldwide spending on cybersecurity was only $3.5 billion. In 2021, cybersecurity spending is projected to total more than $220 billion, according to Cybersecurity Ventures. Microsoft, for example, plans to spend at least $1 billion annually for the foreseeable future, and the US Government budget for cybersecurity for 2019 was $15 billion.

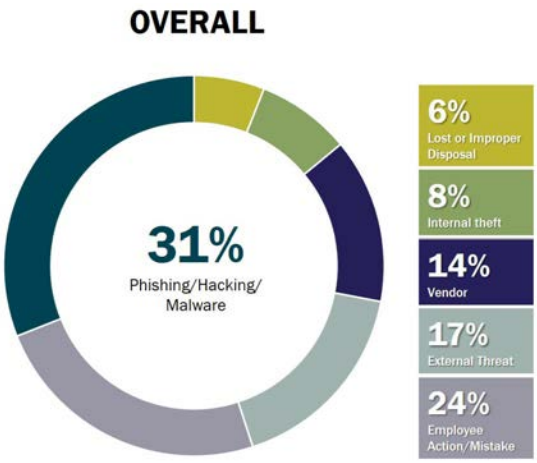
> **"In 2021, cybersecurity spending is projected to total more than $220 billion"**

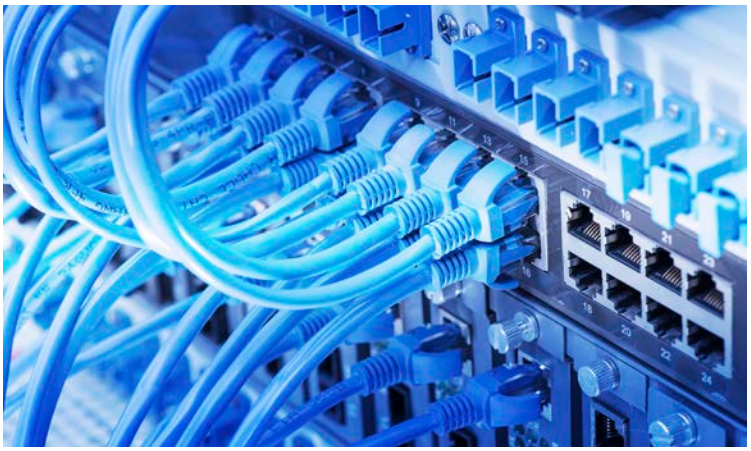
What is all that money being spent on? Cybersecurity is comprised of technical precautions that include:

- Network Intrusion Detection Systems, logging and monitoring,
- Email filters,
- Network Intrusion Prevention,
- Network architecture considerations
- Multi-Factor Authentication

However, cybersecurity isn't threatened by computer hackers alone. In fact, the greatest threat to corporate or government networks is now the human factor. Bad actors send millions (if not billions) of emails (called "phishing"), trying to entice employees to open an attachment, visit a harmful website, provide their

network credentials, or otherwise breach corporate defenses. System administrators and those with elevated network access are generally well-trained and not likely to fall for these schemes, but a small percentage of people will respond (even a fraction of one percent is all it takes). A hacker can use this access to get a small foothold into the organization– an email from an employee or familiar name has a greater chance of fooling others. Another round of emails or requests go out, and more people are fooled. In this iterative manner, the bad actor gains greater and greater access to network resources. They then are able to plant Trojan horses, viruses, worms or root kits to spread their control throughout the network, looking for data or simply infecting wide swaths of digital property. Therefore, while technical protections are important, increasing numbers of companies are training end-users to identify and avoid these early attempts at a foothold into the corporate network are where many companies are focusing their attention. That training is vital, as 70 percent of companies suffered an accidental internal breach within the last 5 years.





"...Another major concern for industries that rely on classified information, trade secrets or intellectual property..."

While phishing is rampant, there are several other threats against your corporate digital assets. Another major concern for industries that rely on classified information, trade secrets or intellectual property to maintain a competitive edge is the "insider threat." An "insider" is an employee or contractor that you have entrusted with access to your system and information in order to perform their duties. However, if that employee's motivations change during the course of employment (or if their motives were not uncovered upon being hired) he or she has much greater access than an outsider, and can cause severe damage to systems, data, and reputation. And, in the case of government clandestine operations, insider threats could put lives at stake.

What do Hackers want?

What do the hackers want? When hackers get into a system, they may perform many different functions. Ransomware is the act of encrypting data and holding the decryption key for ransom. However, data may simply be stolen and/or destroyed. In the case of healthcare information or access to bank accounts, the information may be used for other acts. The hackers may install additional software on systems to allow future access or to perform functions remotely. Hackers are not necessarily looking to "con" individuals out of money. While financial benefit through ransom, blackmail, or other tricks soliciting money is often the primary reason for hacking, there are other reasons as well:

- Just to show they can
- Stealing intellectual property
- Building an army of bots to attack other targets, or to mine for cyber currency, and
- Political, personal or revenge motives.

Are we doing enough to protect ourselves?

Are we doing enough to protect ourselves? According to a Cisco whitepaper, only 32 percent of businesses carried insurance to recover from cybersecurity incidents. Large firms may be self-insuring, but mid-sized and smaller firms cannot afford to do so. IBM and the Ponemon Institute estimated in 2016 that the average cost of a data breach was $7 million; however the hacks against Sony Pictures, Target, and Equifax cost those companies hundreds of millions of dollars. In addition to the monetary cost, cybersecurity threats also impact firms' reputations and the trust of their customers.

What can we do to protect ourselves? The top five ways to protect systems from cyber-threats include:

1. Train employees to be aware of social engineering and phishing methods,
2. Lock down servers – physical and cyber precautions,
3. Deploy a secure network architecture,
4. Implement the principles of “Least Privilege” and “Separation of Roles,” and
5. Monitor security logs regularly.

As we become even more reliant on computers to perform both work and everyday tasks, cyber-threats will likely continue to mount, making these and other protective measures even more valuable in the years ahead.

Adam Shane, PSP, MSEE
Systems Integration Manager
ashane@burns-group.com
www.burns-group.com