Unclear but present danger

Brunswick's MARK SEIFERT and SIOBHAN GORMAN explain that the breach you dread may come from an unexpected source

Security technology company McAfee has reported that its "malware zoo" – where it logs all the malicious software, or malware, it discovers – has grown at last count to 433 million species, around 70 percent more than the previous year. While it is hard to forecast what cyber attacks and cybersecurity will look like a decade from now, it is a safe bet that McAfee's zoo will continue to welcome millions of new, and increasingly nasty, predators each year.

Yet 44 percent of organizations polled by software company CyberArk in 2015 believed they could keep cyber attackers off their networks entirely. In an environment where new threats emerge, evolve and proliferate at increasing speed, this level of confidence is alarming – and reckless.

Cyber threats pose a risk not just to security, but also to reputation. A strategy to address these risks has to acknowledge the likelihood that company defenses will be penetrated, and it should include plans for a response when the attackers gain access to company systems.

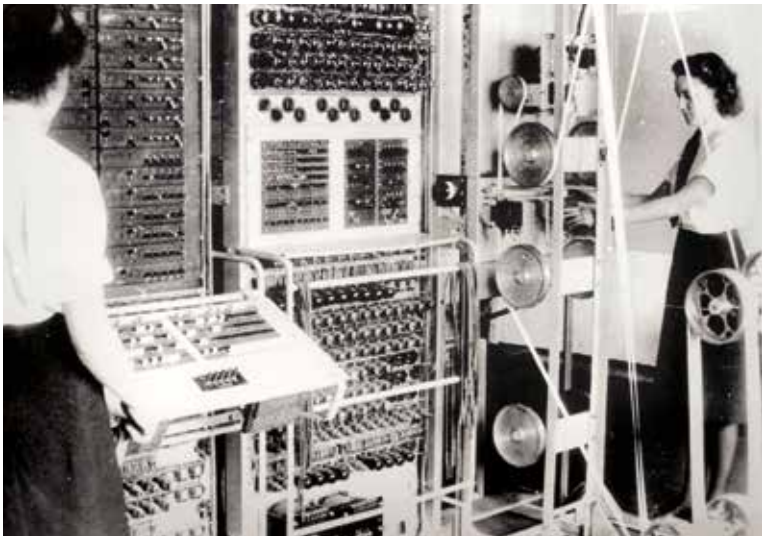
One of the fastest-growing forms of attack globally is "ransomware," where a hacker locks a user out of their data until a ransom is paid. McAfee reported more than 4 million types of ransomware in 2015, 1.2 million of which were new. "Never before in the history of humankind have people across the world been subjected to extortion on a massive scale as they are today," said Symantec, a software security company, in a report on ransomware.

The total cost of these attacks extends well beyond the ransoms paid, says Keith Jarvis, a senior researcher at SecureWorks, a global information security company. Jarvis says the bill "likely extends into the hundreds of millions of dollars annually," after factoring in business disruption and lost data. Each of the most prolific types of ransomware can be responsible for millions of spam emails, Jarvis says. At one time, individuals were most at risk. Now the targets are large and corporate: hospitals, law enforcement agencies, energy companies and even school districts.

Whether in search of publicity or as a tactic to apply pressure, ransomware attackers may tweet their demands. Once out in the open, companies will face questions from investors, employees, customers and law enforcement. Those who are unprepared may have to scramble to formulate answers and coordinate a response while locked out of their emails and internal networks.

Ransomware can become especially complicated in jurisdictions such as the US, where it is illegal

4. COLOSSUS (CODE BREAKER)



PHOTOGRAPH: BLETCHLEY PARK TRUST, GETTY

Colossus was the name given to computers built by the British during World War II to decode the Lorenz cipher, a code used by senior German officers that was even more complicated than Enigma, which Alan Turing had helped solve. Lorenz was first compromised by human error (see "The heart rules the head," Page 14). Colossus went on to analyze and decipher massive volumes of coded messages. Designed by Thomas H. Flowers, who was influenced by Turing's work, Colossus is considered the first large-scale electronic computer – before that, machines had been solely electro-mechanical. Pictured above, Royal Naval personnel operate a Colossus computer in 1943 in Bletchley Park, British code breaker HQ.

to pay money to any person or organization on a terrorist watch list. While such demands are often linked to organized crime, some terror groups may use ransomware to finance their activities. If the attack succeeds, and a company chooses to pay, it should work with specialists and law enforcement to avoid legal or reputational fallout. In addition to technology-based defenses, companies can also educate employees to avoid "phishing" attacks, the most common vehicle for this kind of malware.

ATTACKS THAT MANIPULATE

or compromise data are another growing threat. James Clapper, US Director of National Intelligence, says data manipulation will soon become the most dangerous form of cyber attack facing businesses. "Decision making by senior government officials, corporate executives, investors or others will be impaired if they cannot trust the information they are receiving," he told the US Congress in 2015.

Manipulated data poses significant risks both to individual businesses and to the broader marketplace. If your data can't be trusted, how will customers be able to trust you? What decisions will you be able to make with confidence? Perhaps most frightening of all: what happens if you don't even know that your data has been changed?

Attackers unable to breach your defenses may instead focus on your business partners. Target's highly publicized breach in 2013, when roughly 110 million customer records were compromised, began with an attack on a third-party vendor.

The following year, Benjamin Lawsky, one of New York State's senior financial regulators, sent a letter to dozens of banks requesting information about third-party service providers. "It is abundantly clear that, in many respects, a firm's level of cybersecurity is only as good as the cybersecurity of its vendors," Lawsky wrote. The data agrees with him. In its 2015 Global State of Information Security Survey, PwC found breaches attributed to business partners climbed 22 percent.

Vendors performing mundane functions can often be found to have unexpected and worryingly high levels of access to a company's network. Imagine explaining to your customers why you allowed a copy machine vendor access to their data. Companies should consider cybersecurity when selecting business partners and regularly review those they already work with. What third parties have access to your networks, and under what conditions?

> "Imagine explaining to your customers why you allowed a copy machine vendor access to their data"

Many companies store data and run business-critical operations and applications via the cloud. This is cost-effective, efficient, and can provide a more secure system than many businesses can create on their own. But, as is true for all modern technology, the cloud is not immune to attack.

A hacker need only piggyback on one of the hundreds – or thousands – of businesses using the cloud to attempt to gain access. Once inside the cloud, the hacker can then launch a distributed denial of service attack, overwhelming the system by flooding it with requests from within and crippling the operations of all the cloud service provider's users. The fallout could be disastrous for any business and create a legal and communications minefield.

At this point, things can get very complicated. Some companies might wish to keep the matter quiet; others may prefer to go public. Meanwhile, an investigation by the cloud service provider could raise further questions of privacy, since it might need access to a company's data in order to determine the extent and nature of the attack.

Affected companies might be tempted to blame the cloud-hosting service, but doing so runs the risk of appearing to shirk responsibility. Suing the cloud provider is an option, but that might fuel further public attention and controversy.

COMPANIES CANNOT IMMUNIZE

themselves from these threats. However, the damage can be mitigated if some precautions are taken: have a crisis response in place for each scenario, run cyber attack simulations, educate and train employees, analyze and tackle your vendors' vulnerabilities, and bolster cybersecurity measures. Even simple steps, such as stronger authorizations for data access, can help, and should be a part of a regular review of cybersecurity practices.

Instituting best practice well in advance puts a company on a firm footing should it need to explain or defend its actions in public. "We did all we could," is always a much stronger response than, "We didn't see it coming."

MARK SEIFERT is a Partner in Brunswick's Washington, DC office and co-leads the firm's Cybersecurity and Privacy practice. **SIOBHAN GORMAN** is a Director in Washington, DC and advises on public affairs and crisis, with a focus on cybersecurity and privacy.