Office Locations

Austria

Belgium

Brazil

Canada

Chile

China

Finland

France

Germany

Italy

Netherlands

Norway

Poland

Russia

Spain

Sweden

Switzerland

Turkey

United Kingdom

United States

Daubenspeck and Associates

IMD
INTERNATIONAL SEARCH GROUP

A Rising Tide

Daubenspeck and Associates
July 2017

Daubenspeck and Associates, Ltd
www.daubenspeck.com
(1) 312-297-4100

Daubenspeck and Associates

Two Prudential Plaza
180 N. Stetson Avenue
Suite 1935
Chicago, IL 60601
312-297-4100
www.daubenspeck.com

Epilogue

Despite the speed with which attackers have demonstrated ability to bypass security controls, the cybersecurity industry continues to market products as being "solutions". In practice, without the right people, an organization will always be vulnerable, regardless of how much is spent on security products.

The WannaCry Ransomware Epidemic

The most famous group of hackers in the world may be the group that calls itself "The Shadow Brokers". If you think that sounds like the name of a science fiction villain, that's because it is. The Shadow Brokers are named after a character from the video game series *Mass Effect*. But while their name is silly, the damage they have caused companies is serious. Using a virus called "WannaCry", a group of cyber criminals have weaponized the The Shadow Brokers' work to attack hundreds of thousands of computers worldwide.

WannaCry is a type of malicious code referred to as "Ransomware" that takes advantage of a security flaw—called an "exploit"—found in Windows systems. Once a computer is infected, all of its data is encrypted. The computer then displays a message promising to restore the data if a ransom is paid. If payment is not made quickly, the ransom price increases. If the user still refuses to pay, WannaCry renders the data unreadable. Thus far, the criminals have made over $140,000 from those who have decided to pay the ransom.

The exploit used by WannaCry—codenamed *EternalBlue*—was discovered by the NSA. They kept it secret so that they could use it, only for the The Brokers to steal it from them. Not a humble group, in April 2017 The Brokers brazenly showed the world their discovery. The exploit would be weaponized less than a month later: WannaCry began its rampage on May 12.

Much of the damage caused by WannaCry—a type of Malware called a "cryptoworm"—was avoidable. Microsoft discovered and released a fix for the vulnerability exploited by *EternalBlue* in March. Unfortunately, because many companies fail to regularly update their computers, hundreds of thousands remained vulnerable. Further, systems using Windows XP didn't receive a fix until the severity of the problem became clear. Unless protected by a cybersecurity service, these computers had no defenses.

Thanks to WannaCry's ability to spread through internal networks, businesses and governments are the most at risk. The UK national health service (NHS) was WannaCry's first major victim. It had to cancel medical services after losing access to patient records. Later, Spanish telecom giant Telefónica saw employees from Brazil to Germany get locked out of workstations. FedEx's logistics operations were disrupted. Germany's national rail service lost access to its passenger information. Over 500,000

computers have been affected since May; for the vast majority, there is no way to decrypt affected files. Once infected, it's too late.

The initial method used to stop WannaCry's rampage did not create a positive picture of the modern cybersecurity environment: The worm's progress was first slowed accidentally, after a 22-year-old British analyst purchased a domain he saw was being used by WannaCry. As one cybersecurity expert explained: 'The spread of the ransomware slowed because a researcher found a bug in the malware, not because companies have good security practices'. The hackers quickly altered WannaCry's code to circumvent the fix.

The Cyberthreat Environment

WannaCry is one of a growing number of corporate cyberthreats. In 2016, hackers stole $101 million from Bangladesh Bank. Only $38 million was recovered. In 2013, the hard drives of tens of thousands of South Korean banks and media agencies were wiped without warning. In 2011, Dutch drug traffickers used Belgian hackers to co-opt shipping containers for smuggling.

Cyber vulnerabilities can be systemic. In February 2017, over 150,000 printers worldwide were hacked simultaneously, including office and restaurant receipt printers. The mastermind was a British high school student. Luckily for the "victims", the student did nothing more than use the printers to print mocking suggestions that their owners take network security more seriously.

Tools for hackers are widely available, and hacking services can be bought at a range of prices. Some exploits sell for big money: A major Google Chrome exploit can sell for over $200,000. Google once offered a legitimate French firm $60,000 to reveal an exploit, only for the firm to respond that it could get a higher price elsewhere. Internet Explorer exploits can fetch $500,000.

The internet remains a rapidly evolving threat environment, and it's impossible to guarantee cyber safety. Most coders make an estimated 50 errors per 1,000 lines of code. Some of those errors create security problems. Symantec's study of software released with security vulnerabilities found that it took an average of ten months after release for software developers to discover their vulnerability. Some exploits survive longer—*EternalBlue* worked on operating systems that came out in 2002, but it wasn't discovered and patched until 2017.

The proliferation of exploits is worsened by an industry culture that thinks it's more important to release software by deadline than to ensure that a product is free of errors. Computer security expert Ross Anderson describes this philosophy as "Ship it on Tuesday, fix the security problems next week—maybe". Because each new edition of software contains new code, a new vulnerability could be coded-in at any time. There's no such thing as a dependable brand.

Further, a company with secure systems can be made vulnerable by the third-parties they work with. In 2013, hackers stole credentials for Target's computer systems from the air conditioning company that Target had contracted. This gave the hackers "legitimate" access to Target's point-of-sale systems, which they used to steal the credit and debit information of 40 million customers. Like with all facets of business, in cybersecurity it's 'who you know' that matters.

The Rise of New Threats

Experts agree that cybersecurity threats are a permanent hazard. Further, the internet remains a rapidly evolving threat environment. Securing a computer to keep out cyber criminals is as necessary as locking a door to keep out regular criminals.

Rates of ransomware infection are rising fast. A negligible issue as recently as 2014, between 2015 and 2016 the rate of ransomware infection increased 36%, and the average ransom demand more than tripled. Between January 2016 and December 2016, Symantec's rate of detected ransomware attacks rose from 846 per-day to 1,539 per-day. WannaCry has made 2017 the worst year for ransomware yet.

Over a third of all ransomware attacks target the United States, with Japan coming a distant second at 9%. This is possibly because Americans are far more likely to pay ransoms than individuals from other countries—64% of Americans pay, compared to a 34% global average. Attackers increasingly combine ransomware with malware designed to figure out how much money they can extort from their targets, but only 34% of those who pay get their files back.

Business email compromise (BECs) attacks, commonly called "spear phishing" scams, are a fast-rising threat to business. BECs are targeted attacks that utilize social engineering techniques to scam employees. In BEC scams, cybercriminals impersonate a company executive or other key individual through a compromised email account. From there the criminals order fraudulent wire transfers, invoices, and steal data. In 2016, Austrian aerospace manufacturer FACC fired its CEO after the company lost $47 million to a BEC scam.

The growth rate of BECs is astonishing. In June 2016, the FBI released statistics which showed that the rate of BEC attacks had increased by 1,300% since January 2015, and that attackers had used BECs to steal over $3 billion internationally between October 2013 and May 2016. Six months later, an update showed that the amount of damage had risen to $5.3 billion, and the rate of attacks was now over 2,300% higher than in January 2015. The chief victims of these attacks are U.S. companies.

The rise of BECs emphasizes the level of threat that can be posed by a single compromised individual. Texas-based manufacturer AFGlobal lost $480,000 after its accounting director was duped by a BEC scammer who impersonated both the company's CEO *and* their KPMG-based attorney. If a company doesn't train its employees in procedures designed to prevent the fraudulent use of legitimate credentials, even the best protection can be useless.

The Danger of Data Breaches

Computer data breaches are a significant threat to business. Over the next 24 months, companies in the United States have a 24% chance of experiencing a data breach that exposes at least 10,000 records, according to the *2016 Ponemon/IBM Cost of Data Breach Study*. U.S. breaches have the world's highest average cost ($7.01 million), including the highest cost due to reputation damage and lost customers ($3.97 million). The EU's General Data Protection Regulation, which come into force next year, (2018), while only impacting organizations holding personal data on EU citizens, will also impact the subsidiaries of many US multinationals.

The Ponemon study also found that 65% of data breach costs are indirect costs such as damage to reputation. 48 states require companies to disclose breaches to clients and investors. Due to a

combination of fines, information sensitivity, and customer mobility, indirect costs are even higher in regulated industries. Financial firms face an average customer churn of 7.3% after a data breach.

The threat is severe for all sizes of business. According to a Keeper-Ponemon survey of firms with between 100 and 1000 employees, 55% had experienced a cyber-attack in the last 12 months, and 50% reported a data breach. These incidents cost an average of $879,582 due to damage or theft of assets, plus an additional $955,429 due to operational disruption. Yet many companies report doing little to guard against breaches.

CSID, an identity protection company, found that 62% of firms with less than 10 employees don't regularly update their software, and 38% don't take any precautions whatsoever. But these businesses don't escape the notice of hackers: 43% of targeted attacks in 2014 were aimed at a small business, and one in every 127 emails sent to businesses with between one and 250 employees is malicious. That rate is higher than many larger-sized firms face.

Cybersecurity threats have proliferated as increased connectivity has increased the market incentives to gain and sell the skills necessary for cyber-crime. As this market proliferates, the cost to purchase services decreases. It costs just $25 to buy password stealing software online. The growth of 'contractors' offering "Crimeware as a Service" (CaaS) allows a criminal to simply choose a target and a goal, and the contracted hacker will do the rest.

The price of a data-breach can be enormous. The average cost of a single stolen or lost record is $221. How many records does your business have? How many of them can you afford to lose access to? What will your clients think if you lose their data?

Mitigating Threats

It is impossible to fully safeguard against all cyber-threats. Human error remains the ultimate vulnerability, and if the NSA can be compromised then so can you. Further, many companies experience attacks that bypass intrusion detection and antivirus software. Mandiant, a cybersecurity service arm of FireEye, estimates that most companies don't discover an intrusion for over seven months after it happens. It is vital that companies have the training to respond swiftly to a cyber-attack.

Every business should develop a plan to recover from breaches. A company that can't respond to an attack is like a body without a functioning immune system. Implement a business continuity management (BCM) plan to ensure that your costs stay manageable should your cybersecurity fail. BCMs reduce the cost of a data breach by 15%, and reduce the likelihood of one occurring by 29%. There are numerous steps that you can take to manage breaches.

First, in the event of a breach, you can reassure your clients that their data is secure by using encryption software to protect your data both in-storage and in-transit. Customers may look favorably on companies that take preemptive steps to protect their information: Encryption can lower the cost of a data breach by an average of $19.90 for every lost or stolen record.

Because attacks can damage your data, ensure you have backups. Because a comprehensive compromise of a network can include the on-line storage solution, off-line backup of critical data is needed. Cloud-based services such as Acronis will automatically backup your entire system. You can also use external hard drives and memory sticks to have employees save data on an individual basis.

This strategy is effective with policies that only allow computers to accept pre-approved external media. External storage is increasingly cost-effective: 64 gigabyte memory sticks sell below $50.

Finally, consider purchasing cyber insurance, a relatively new facet of cyber-protection. PricewaterhouseCoopers estimates that over 30% of American businesses have some level of cyber insurance. These policies often offer only limited guarantees, but the market is evolving rapidly. Some cybersecurity services, such as SentinelOne, include insurance as a guarantee against losses should their services fail.

Preventing Threats

A computer network is like a building with multiple doors and windows that cybercriminals can try and enter through. A comprehensive and multi-layered approach to security is required to protect your network from cyber-attacks.

The most basic way to protect yourself is to keep your system updated. Implement a schedule to embed accountability into the process; designate one day a month to update your software. Exploits for Windows vulnerabilities can appear very quickly, so Microsoft's advice is to turn on automatic updates for any non-critical systems. Out of all the companies hit by WannaCry, none had up-to-date computers. Updating can feel inconvenient; but WannaCry's victims would have been saved endless grief had they kept Windows current. (And remember: Anti-virus software and firewalls won't protect your computer if they're out-of-date too.)

Cybersecurity software is vital, but no form of security can protect against human error. Your biggest tools for preventing a security breach are employees trained in safe computer use. Studies have shown that employee education is associated with a significant decrease in the costs associated with data breaches. Cybersecurity services should be a backup, not a first resort. You wouldn't leave the door to your house open just because you have ADT.

Attacks such as BEC scams rely on exploiting both computers and humans. An employee who opens the wrong email attachment could infect your entire network. Mitigate this risk by teaching standardized computer use policies. These include setting password security standards and verification procedures for handling any email with unexpected attachments or password reset requests.

Bolster your email security further through use of an authentication service to ensure that emails are not coming from imposters. Most major cybersecurity and email service providers offer these services. You can augment them with a policy that requires employees to verify any unexpected requests to transfer funds or alter financial information.

Finally, make sure that employees and contractors don't have more permissions and access than they need to do their job. Target's point-of-sale systems would never have been compromised had its air conditioning company not been given unnecessary access to them. The amount of damage that a hacker can do with a single employee's login details should be limited.

Conclusion

For fully effective computer security, cybersecurity must be seen as a "public health" issue where safe usage procedures are a whole-of-company practice. Employee education should create "buy in" to the

belief that cybersecurity procedures are intrinsically worthwhile. Effective cybersecurity should not be presented as an "extra"; rather, if an employee fails to practice effective cybersecurity it should be seen as negligence: Given the large amount of business that companies lose due to data breaches, it appears that the public already sees it this way.

About Daubenspeck and Associates

Daubenspeck and Associates is an international retained executive search firm. Based in Chicago and founded in 1982, Daubenspeck and Associates, Ltd. is a privately held corporation. Known for combining a global reach with a personal touch, Daubenspeck and Associates is an expert in executive search, cross-border appointments and culture match. A Top-40 Search Firm with executive leadership identified by BusinessWeek as one of the "150 Most Influential Headhunters in the World," Daubenspeck and Associates is a member of the Association of Executive Search Consultants and the IMD International Search Group.

Daubenspeck has supported countless multinationals in strengthening their cyber security leadership.