Corporate Cybersecurity

A Discernum White Paper

October 2017

Table of Contents

Introduction

The 2017 data breach at Equifax Inc. reminded the American public that some major companies are not adequately prepared to protect sensitive information against cyber-attacks. Equifax, a major data aggregator and consumer credit reporting firm would reasonably have been expected to have state-of-the-art cybersecurity policies and practices in place. The theft and likely subsequent misuse of the information held by Equifax has the potential to undermine the entire American system of consumer credit. As a byproduct of that undermining, the entire United States (U.S.) financial system may be irreparably harmed. All of this is in addition to the emotional impact at the individual level, where Americans whom have fought hard to build and maintain good credit could have all of that effort go to waste. Victims could go into great debt due to loans taken out by identity thieves, in part thanks to the irresponsibility of Equifax.

The purpose of this research was to examine what cybersecurity policies and practices can be reasonably implemented by corporations to reduce the incidence of similarly devastating attacks from occurring again in the future. The concluding recommendations attempt to avoid highly technical, sophisticated cybersecurity measures that require a deep knowledge of web technologies and programming languages to implement. Rather, the goal was to generate research-based recommendations that can be implemented broadly, and possibly even by those with only a moderate level of technical expertise, yet still have a strong impact on the security of digital assets. If successful, these actions will not only have a positive impact on corporations, but also consumers that all too often become unwittingly victimized.

State of Affairs

The 2017 Verizon Data Breach Investigations Report (VDBIR) summarizes key points on data breaches that occurred within the year of 2016. The summarized points include who conducted the breaches (e.g. internal or external actor), general tactics that were used, victim makeup, and other commonalities between attacks. Verizon has released this annual report for ten years now and it has become a respected source of information within the professional cybersecurity community. The VDBIR has been used throughout this report's research as a source of quantified data on cyber data breaches. In addition to analyzing the broad level data in the VDBIR, some recent major cybersecurity incidents were also individually reviewed.

Verizon Data Breach Investigations Report Key Data

The 2017 VDBIR found that 75% of attacks in 2016 were perpetrated by outsiders, whereas the remaining 25% directly involved insiders. More than half involved organized criminal groups and/or state actors. Nearly two thirds of attacks involved technical hacking, more than half utilized malware, of which two thirds was sent via email attachment. The amount of malware received via email far outweighed that encountered via web browser, perhaps because email is addressed (targeted) to a specific victim. Further information in the VDBIR indicates that 43% of breaches involved various types of social engineering attacks, and an astounding 81% of attacks exploited compromised passwords. Only 8% of 2016's attacks

involved the physical presence of the attackers when committing their breach, alluding to issues of attribution.

A Review of Recent Cybersecurity Disasters

Office of Personnel Management Data Breach

The 2015 cyber breach of the U.S. Office of Personnel Management (OPM) had impact that may not be realized for many years. As a part of the breach, extremely private information was stolen, such as completed government SF86 security clearance forms, applicant fingerprints, and polygraph results. This breach shows us that even governments are not immune to successful attack; and not even when it involves some of their most secretive information.

It is likely that a state actor such as China was responsible for this breach. The attack is thought to have been possible because stolen credentials from a separate breach regarding a government contractor were used to hop over to the OPM's internal network. That breach is believed to have occurred five months before the OPM breach. Once inside the OPM network, the attackers began offloading troves of data until finally having their access cut off many weeks into the attack.

Better staff training may have prevented the OPM hack. Specifically, training on how to properly monitor a network for anomalies. Additionally, employees should have been trained to remove any credentials that were no longer being used, or were possibly involved in a breach somewhere else. Further, when dealing with information as sensitive as the information the OPM was storing, the password portion of credentials should have also been forced to change often. If OPM had been using two-factor authentication, this may have also prevented the breach from occurring, or at least delayed it.

United Airlines Data Breach

It is believed that in mid-2015 hackers compromised the information systems of United Airlines, exposing the travel records of millions of flyers. While minimal information has been released to the public regarding how this breach occurred, the attackers are believed to have used stolen credentials, just as with the OPM hack.

The United Airlines data breach may have also been conducted by the same group responsible for the OPM attack. The information obtained from the United Airlines breach in conjunction with that of the OPM hack would be of great value to foreign intelligence services and governments. United Airlines may or may not have known at the time that they were a likely target of state actors, but a detailed information security risk assessment should have implied so. The airlines fly everyone from the average person to CEOs planning major mergers and acquisitions to government agents handling spies around the globe. To help conceal their identities and support their covers stories, many of these agents travel to third nations prior to entering target nations under cover. Having access to flight records may show that these agents are flying in and out of Washington D.C. regularly. This would draw immediate suspicion and allow a foreign intelligence agency to better direct their targeting and investigative efforts.

The United Airlines breach may have been prevented had information security managers realized the value of the information that they were protecting. This would have occurred during the course of an information security risk assessment. United likely had a working risk assessment, but it is possible that the risk assessment was not thorough enough, or that the resulting security recommendations were not adequately heeded.

Equifax Data Breach

Unfortunately, many of the victims of the mid-2017 Equifax data breach never chose to provide Equifax with their social security number, date of birth, home address, and account payment history. And even those that did reasonably expected their information would be protected by the company storing it.

It is believed that the Equifax breach was possible because company employees failed to properly patch a known vulnerability in their consumer disputes web portal. Once hackers made their way in, they were able to access private information on over 200 million people. Equifax did make attempts to patch the vulnerabilities, though the efforts were unsuccessful. Once in, the attackers had weeks to access and offload private information, much of which may not have been encrypted.

The Equifax breach could have been prevented or mitigated through proper patching of vulnerabilities, two-factor authentication, and better use of encryption. Equifax's information security risk assessment would have informed security managers of the extreme value of the information the company was maintaining. They likely knew they were a major target for data breach. Regular security audits in the form of penetration testing would likely have helped employees keep their guard up and be better prepared to protect the information they were responsible for.

Cybersecurity Practice Recommendations

Having looked broadly at cyber incidents through the research of the VDBIR and specifically at three modern cybersecurity disasters, five key areas have been identified where relatively simple security measures have potential for big impact. They are: Systematic security risk assessment, intelligent authentication policy enforcement, targeted use of encryption, staff training, and recurrent security auditing.

Systematic Security Risk Assessment

Undergoing periodic security risk assessment is a critical step in securing a corporation's assets, and the risk assessment should be the primary driver of the security budget and security plan. If an organization is waiting for a breach before implementing stronger security, and has no working risk assessment, the breach they are waiting for will surely come.

Operating without an updated security risk assessment is akin to firing without aim. Organizations that do not understand their most probable and critical threats, and are unaware

of their major vulnerabilities are operating blindly. The first step to establishing a proper cybersecurity program is conducting a risk assessment.

Another reason that risk assessments are so important is that they help justify the security budget. They also help cybersecurity managers know where funds are best spent; where they will have the most bang for the buck. Just as budgets are generally updated annually, so should the risk assessment be.

Intelligent Authentication Policy Enforcement

The 2017 VDBIR found that 81% of cyber breaches in 2016 involved weak or stolen passwords. Both the OPM and United Airlines attacks involved use of stolen credentials. Humans, like water, look for the path of least resistance. If a customer's account is hacked, the corporation must take some level of responsibility. Regardless of who is directly to blame, the company's reputation is negatively impacted almost any time there is a security incident. To prevent breaches of individual user accounts, two-factor authentication is strongly recommended. This technique can be used for both employees of the firm that may have a high level of account privilege, as well as individual customers of the company. Two-factor authentication uses both something a user has and something they know. Because of this, it will even reduce the chance of a breach when an account is using a very poor password such as "12345".

Within a corporation, an employee's access is often more sensitive than believed at first glance. For example, a low-level admin might not be dealing with critical information, and the information technology department may not feel the need to enforce strong password policy on this class of employee. But if later the admin needs to work remotely, they may be given virtual private network (VPN) access. If they use a simple password and their VPN access is compromised, the attacker now has a remote tunnel into the internal network.

Intelligent authentication policy can enforce both two-factor authentication and strong passwords. The authentication server should also be set to force a password change at regular intervals, so that if an attacker has made their way inside, their access lifetime is limited.

Targeted Use of Encryption

No matter what someone does to secure a system, there is always the chance that a breach will occur. The Equifax breach reminds us that attackers may be able to access a system even at the government level, and steps must be taken to protect information on that system even once the outer layer is breached.

Companies should plan to be breached; they should assume that their networks will be compromised by sophisticated attackers. Knowing that this will happen, they should have internal data encrypted with credentials separate from those required to access the network, including network admin credentials. They should also have policy in place where old and irrelevant data is permanently deleted, even if it is encrypted. This will reduce the impact and loss size if and when a successful attack occurs.

In the VDBIR report it is noted that 30% of 2016's data breaches in the healthcare industry were the result of non-malicious mistakes such as lost laptops. This is further evidence that employees must be forced to use full-disk encryption. Arguments that encryption is a waste of time because it can sometimes be broken are flawed and show evidence of failing to understand the concept of defense in depth, where multiple overlapping layers of security come together. No single chess piece can win by itself.

Staff Training

Aside from conducting security risk assessments, training is arguably the single most important practice when it comes to reducing the likelihood and impact of cyber-attacks. Humans are the weakest link in most security systems. If software has no holes, and passwords are so strong they are unable to be brute forced, attackers will often decide to target the human element. These attacks use social engineering and other psychological tactics to totally bypass digital and physical security controls. Two-thirds of the malware deployed in cyber-attacks was distributed via malicious email. That means two-thirds of cyber-attacks may be preventable through employee training, which can include training on how to recognize and deal with suspicious email.

Staff should be rewarded for reporting suspicious activity such as email phishing. This sort of encouragement may create a culture of awareness, and remind employees of the importance of reporting potential security issues. Another area where employees should be given positive reinforcement is for finding outdated or unpatched software and helping to rectify the issue.

Looking beyond corporate staff, one major U.S. bank is distributing high quality cybersecurity literature to customers that is both informative and easy to read. This bottom-up approach has the potential for significant impact. That said, helping the consumer to be more cybersecurity aware does not relieve corporate employees of their responsibility to protect the data they profit from maintaining.

Recurrent Security Auditing

A grand plan may have been developed, and tens of millions of dollars pumped into security, but a corporation must test their plans. An untested security plan should be assumed to be an ineffective one. Security audits are the checks and balances that keep a security system effective in the real world.

Imagine a company developing a bullet resistant vest and then never firing a shot at it. They assume that because the vest is made from the same material as the other vests they have been selling for the last decade, that this new vest will work too. What they did not account for was that the bad guys were now commonly using a new type of ammunition on the market that could easily penetrate the old style of vest. Had the company actually tested their new bullet resistant vest against modern ammunition they would have realized that their plans were in dire need of updating.

Another advantage to security audits is that they reduce complacency on the part of information security staff. For staff that have never experienced a major breach it is easy to become complacent and start to believe that a breach will never happen on their watch. They

may also not be thinking of creative yet realistic attack methods that an outside red-team or penetration test team may be well versed in. Once they experience a mock breach from a security audit, the threat becomes more real to them. Most people do not like to be defeated, even if in a game. A security audit is a war game that staff play together to prepare themselves for encounters with real world threats. Had the OPM, United Airlines, and Equifax played more war games, perhaps they would have avoided their major cybersecurity breaches.

Conclusion

There are many commonalities in attack methods used throughout most recent cybersecurity breaches. The cybersecurity policy and practice recommendations presented here are intended to be effective in the majority of corporate situations, and relatively easy to implement. They are meant to cause minimal inconvenience to the company, and avoid extreme cost. They are by no means a total package, though they are a good start for any company beginning to take cybersecurity more seriously.

There are a number of other recommendations that a comprehensive security plan should include, depending on resources available to the organization, and threats faced. The OPM was likely targeted by a state actor, and if they had not gotten into the network via the means that they did, they likely would have continued attempting via different avenues. The information that OPM was maintaining was of such extreme value, that certain threat actors would likely have been willing to spend a great deal of resources on accomplishing the breach. A proper risk assessment should have shown this. When the risk assessment shows that assets are that valuable, sometimes more extreme measures must be taken, such as using dual encryption, system-wide multi-factor authentication, and keeping certain information completely disconnected from the internet. Measures such as these may be inconvenient, but strong security does often require users to work a bit slower or less efficiently. These are the simple facts of security versus convenience.

The results of this research are simply a starting point; a way for organizations to get a basic cybersecurity plan off the ground and provide the necessary protection to their organization. If they start moving through the risk assessment process and realize that their security plans are inadequate, they must revisit those plans.

The major data breaches of the last few years should serve as a wakeup call to corporations: They must not idly stand by until they are successfully breached to begin implementing effective cybersecurity.