INDUSTRY INSIGHT / DARREN KRUK

Adapting to new information security threats is critical to survival.

Long before Darwin's theories and his book *Origin of the Species* was released, humans realized that the key to survival was adaptation. When the environment changed, those who were able to change along with it survived, those who were not perished. In today's age of electronic communication, virtual meetings, cyber wallets, and cyber terrorism, the validity of the statement is acknowledged, and the realization that companies need to be more vigilant protecting their electronic environments. Those companies in high-profile industries such as finance, aerospace, military, and others–including housing and mortgage servicing—need to be more aggressive as the risks are generally higher when handling and storing confidential data.

CRYPTOGRAPHY HAS A LIMITED LIFECYCLE

Given the massive data breach Equifax experienced recently, implementing encryption algorithms—or the process of transforming plain text into encrypted text for the purpose of securing electronic data when it is transported over networks—based on the lowest strength encryption that has not yet been exploited may not be the wisest course of action. It does not make sense to base security protocols on the lowest level of Federal Information Processing Standards (FIPS). If companies are adopting new controls based on today's industry encryption standards, they should have a valid reason for doing so, and understand the implications of that decision. After all, the time involved in the decision-making process can be quite extensive. There is research that takes place to evaluate the issue, requirements and design, RFPs, testing, implementation, and more. This can be a costly process and companies should not exhaust all the time and resources necessary only to adopt algorithms that are here for a short period. They should be implementing protocols that will not be deprecated for at least the next eight to 10 years. This is one of the reasons why certifying authorities such as Verisign, Thawte, and others limit the number of years users may purchase a website certificate. Major institutions may only implement certificates whose expiration date is two years or less.

When implementing encryption algorithms, companies should consider the effective lifetime of those controls, also taking into consideration the possible time it would take to exploit them. Current standards, such as FIPS, which were developed years ago, are meant as guidelines for security compliance. Those new to security may reference these standards as a rough posture assessment of their systems but

EVOLUTION OF CYBERSECURITY

"Long before Darwin's theories and his book **Origin of the Species** *was released, humans realized that the key to survival was adaptation. When the environment changed, those who were able to change along with it survived, those who were not perished."*

this will only lead to frequent changes of the system's architecture when standards change. For example, FIPS 140-2, which is still used to ensure companies are following proper security precautions, was implemented in May 2001. While there were proposed updates to this standard, they were never adopted:

- January 2005 – Federal Register announced development of FIPS 140-3 Cryptographic Modules
- July 13, 2007 – Federal Register released the draft of Cryptographic Modules
- December 2009 – a revised draft was released
- August 2012 – there was a request for additional comments to FIPS 140-3

This process continued until the FIPS 140-3 update died, likely because some of the recommendations within it were out of date and already compromised. Still information security teams and the companies they work for are left with an antiquated standard of FIPS 140-2.

There have been thousands of security breaches and advances since that time, yet to be compliant, companies merely need to meet a 16-year old standard. To survive the onslaught of cyber attacks that continue to plague all industries, companies must be increasingly more vigilant. Do not wait for standards to be set for the industry but adopt tougher security protocols, encryption algorithms, and procedures before the current ones are exploited.

In an industry like mortgage servicing where the compliance and regulatory requirements have changed dramatically since the 2008 mortgage crisis—including increased oversight and reporting of breaches—what are companies that support the industry, like mortgage field services, to do? Adopt a security-centric view of the industry and monitor, adapt, and react quickly to changes. The mortgage field services industry has an opportunity to help lead the way for its mortgage servicing clients, rather than waiting for directions from them on security protocols.

PARTNER WITH BUSINESS/OPERATIONS

An important lesson that can be learned from larger corporations regarding security is that they have already adopted the practice of including security advisors at their decision-making tables. New initiatives should go through a threat management evaluation in the same way that they are evaluated for fiscal viability and feasibility. If adding that new functionality to an application could compromise security and expose the company to the possibility of a breach, is it really worth the consequences? Regardless of the answer, the important concept is the evaluation process. Companies need to understand and weigh the implications of their options, good and bad, to reach an informed decision. In many organizations, security is still viewed as a necessary evil, rather than as a welcomed partner. In part, this is because security is often seen as an obstruction to new functionality in information technology. When properly aligned with other business interests, the offering of alternative, secure ways to implement business objectives actually foster the collaborative and beneficial relationship.

MONITOR AND STAY VIGILANT

A large part of the critical security process is staying up-to-date on the latest trends and vulnerabilities. In the past 10 years, there has been a growing segment of the information security industry that offers services ranging from incident response retainer to virtual chief information security officers (CISOs), and

of course, monitoring needs. These external companies have highly qualified and experienced staff that can monitor network traffic reactions to possible intrusion. They offer an alternative to an in-house-developed Security Operations Center (SOC) for those organizations that do not have the expertise themselves.

Regardless of how monitoring is accomplished, it is imperative that it takes place. Internal monitoring via security information and event management (SIEM) can give a holistic view of a company's network and systems, and alert security officers to anomalies and suspicious activity.

Monitoring of threat activity is as important as the monitoring of internal events. To determine if the various software and systems that are deployed within a company's environment are vulnerable to attack, it must be aware of the versions of code and firmware it is running. Remember to review all of the company's systems and software, old and new. While new code may have a few bugs, often-new vulnerabilities are found within very-old code that has been used successfully for years. There is greater risk with the older code because new software is regularly built on old code libraries and segments, and companies may be unknowingly susceptible to the exploits.

There are numerous services and websites that can be used to identify the latest breaches, attacks, and vulnerabilities. Some of these sites include:

- US-Cert.gov
- Exploit-DB.com
- Sans newsbites and @risk
- Nist.gov
- ZeroDayInitiative.com (announcements for zero-day vulnerabilities are on their Twitter feed)
- DataBreachToday.com
- Snopes.com
- Symantec.com
- Various manufacturers' sites

It is important to be aware of new vulnerabilities because once they are discovered, it is only a matter of time before they will be used by hackers to try and compromise unsuspecting networks.

REACT AND REMEDIATE

After implementing all of the proper controls and toughest encryption on the best gear available, it is time to rest easy, correct? Not exactly. As identified in monitoring protocols, there are vulnerabilities found in both new and old code daily. Subscriptions to the cybersecurity lists such as US-CERT and others confirm this, and set off a chain reaction of events that trigger the next course of action—remediation.

Once these vulnerabilities have been identified and posted, companies only have a small amount of time to patch their systems. This is the part where reaction time is critical. The longer systems remain unpatched from new vulnerabilities, the greater the odds that one of these vulnerabilities may affect the business. There are various published standards for remediation time based on the severity of the vulnerability and its prevalence in the wild. The times generally range from several days for zero-day vulnerabilities, and as the severity decreases, the time allowed to patch increases.

Depending on the complexity of applying the necessary patches, firmware, and updates, the company may be vulnerable for longer than necessary. In some cases, companies may opt to wait before applying the patches from fear that they may adversely affect their systems. This is a standard methodology adopted by information technology experts to watch new software and only adopt it once the bugs and inconsistencies have been worked out. But it is a dangerous gamble when racing a clock and betting on the fact that the company will not be targeted.

ADAPT OR DIE

To make assumptions based on the idea that hackers only target large businesses and companies that have high-value data like the mortgage servicing industry is wrong. Examining recent attacks of "wannacry" and "notPetya," the groups that released these did not target individuals but rather sent them out in a wide scope. The malicious actors themselves were unaware of how successful their worldwide cyber attack would be, and were not prepared for the fallout of the attack. Some of the 200,000 victims of the ransomware probably thought that they would have sufficient time to remediate their systems. This is why companies cannot afford to hesitate too long in this new cyber landscape. They should be fostering the security-lead decision-making process and implementing new procedures within these companies to facilitate more aggressive patch cycles, and decrease the amount of time to remediate new vulnerabilities.

Those in the mortgage field services industry know that their servicing clients are well aware of the same vulnerabilities when they are released, and how damaging they can be. These clients, as part of their own due diligence, are reaching out to their field services partners and requesting posture assessments of new threats. This is why field services companies and their security leaders should not only be first to evaluate, mitigate, and remediate environments, but also take the lead and proactively inform their servicing partners of their positions to demonstrate that they understand the risks, and take them seriously.

EXCEPTIONS TO THE RULE

As mentioned, there are times when it is necessary to maintain deprecated and sometimes older standards, but this should be done with full understanding of the risks involved. There also should be mitigating controls in place to monitor the systems and events for anomalous activity that could be indicative of intruders and malicious software. One reason to maintain old standards is the interoperability with outside parties that have a more complex environment, or are not as agile, and are currently on old standards. Of course while the current situation may dictate this position, companies should have a plan to migrate to supported protocols at the first opportunity. Another case may be to support a legacy framework within a company that is incompatible with the newest protocols. These are only a couple exceptions, and while each situation may be unique, reasons exist for not upgrading as quickly as needed. Those entities that are looking to subvert a company's network and systems are counting on complacency.

The mortgage servicing industry and its field services partners can no longer afford to merely meet security compliance standards, but should aggressively be pursuing a more stringent security posture. When implementing cryptographic controls, companies should opt for the highest common level that their environment can support to afford the most time before change becomes necessary. The cyber landscape has changed from the targeted attacks, and companies need to become more adaptable in preventing them. DS