ACCESS BUSINESS TECHNOLOGIES

Whitepaper

A Cybersecurity Solution for Mortgage Companies

By
Access Business Technologies

February, 2017

I. Executive Summary.

Cybersecurity is *the* hot topic for every business today, whether that business is local or global. In recent years, cybercrime expanded into the global marketplace; for instance, compromising the security codes from a bank in Singapore in order to steal money held in the accounts of a federal bank in New York.

That does not mean, however, that local businesses can rest easy. Even small mortgage company networks face compromise through viruses and worms that infiltrate security measures via infected emails or fake social media ads. No business is immune from hackers intent on stealing sensitive financial and personal information. Just ask the government agencies and department stores who have suffered heists of massive consumer information.

No longer can small businesses count on their size as a protection against attack. The question today for CEOs and small business owners alike is not *if* cyber hackers will attack their businesses but *when*.

Exacerbating this issue is that cyber criminals seem to evolve and become more sophisticated in their attack methods every day. They delight in thwarting the latest security systems with new hacks. They bypass security protocols to hide evidence of malware in victim networks, making it harder to recognize when an attack is imminent. Worms wait for opportunities to self-execute and trojans lay concealed until an unsuspecting person unintentionally triggers the fatal execution command. Cyber criminals no longer seem satisfied with causing interruptions of the work stream and disruptions of service. Now, they extort money.

II. The Cybersecurity Problem

It's hard to overstate the size of the cybercrime problem when a conservative estimate places the number of breaches in 2015 at half a billion personal information records stolen or lost. Security experts estimate the number of reported identities affected in 2015 was 429 million. The problem is potentially greater than that, too, because companies often choose not to report the full extent of successful breaches.

Another problem is that administrators often leave the doors open to cybercriminals by failing to secure their websites from vulnerabilities. Symantec's security experts estimate that almost 75% of all legitimate websites have unpatched vulnerabilities.

All kinds of attacks are on the rise, too. Phishing campaigns increased 55% while ransomware increased 35%. And the targets are changing, too, as hackers carried out ransomware attacks against popular devices like smart phones, smart watches, and smart TVs, as well as Mac and Linux operating systems not considered high targets up until now.

The more connected businesses become, the more vulnerable they are and the more costs continue to escalate. The average cost of corporate data breaches increased to $3.5 million in 2015. To put that another way, on a consolidated average basis, each lost/stolen record of sensitive and confidential information costs $145.10. In the U.S., those costs are $246 per

lost/stolen record. That statistic makes it easy to understand why financial services sector losses from security breaches increased 24% in 2015.

Security breaches are costly in terms of lost time, too. Security incidents caused more than 8 hours of downtime for 31% of organizations.

Some good news. The good news is that companies who report having a strong security protocol also report reducing the cost of breaches by as much as $14 per record. Companies that maintain strong business continuity management policies, reduced their data breach costs by an average of $9 per record.

Mobility costs. As companies increase their dependence on mobile devices (and who isn't in today's digital marketplace), their vulnerability to attacks and stolen information also increases. Symantec's report indicated the following eye-opening statistics:

- Thieves steal one laptop every 53 seconds.
- 70 million smartphones are lost each year, with only 7% recovered.
- 4.3% of company-issued smartphones are lost or stolen every year.
- 80% of a lost laptop's cost relates to data breach.

- Thieves steal 2% of mobile devices from the office/workplace but a whopping 24% from conferences. Implementing and enforcing strong security policies has shown it can reduce laptop theft by 85%.

Other statistics round out the problem. The Bit9 + Carbon Black Threat Research team undertook a ten week study that found five times more operating system malware in 2015 than during the *previous five years combined*.

The Internet Crime Complaint Center reported 2,500 cases of ransomware at a cost to victims of $24 million in the US alone for 2015. In addition, researchers report tracking 500+ malware used to bypass security detection. The average number of evasion techniques used per malware sample is 10. The math astonishes.

More astounding insights: 97% of malware is unique to a specific endpoint, which means that signature-based security protocols become virtually useless. Malicious execution is possible in 15% of new files. Microsoft Office-targeted threats use macros 98% of the time and there was a 50% increase in email attacks where macros are the method of infection. Researchers found a 600%+ increase in attachment-based vs. URL delivered malware attacks from the middle of 2014 to 2015. The AV Test Institute registers 390,000 malicious programs every day.

There is hope. Businesses can realize a 19.2% potential increase in detecting malware simply by adding a second anti-virus program to existing email security, while cleansing or purging dangerous or hidden code in files can help eliminate macro malware threats.

III. Malware: History & Background

When it comes to managing cybersecurity, it is useful to understand the complex mechanisms with which hackers can launch attacks against networks.

Malicious software (known popularly as malware) is a broad term. In general, the term refers to any type of software that hackers use to disrupt computers, computer networks, or mobile devices. Malware can operate as simply as displaying pop-up ads or other unwanted programs which slow down computer systems. On the other hand, more sophisticated malware often gathers financial or other sensitive personal information that it then passes on to third parties for heinous purposes. In the most common occurrence, hackers often use stolen authentication details to gain unauthorized access to networks. The following paragraphs describe various types of malware.

A factor to bear in mind: hackers deliver 66% of malware via infected email systems.

Computer Viruses

Computer viruses work to infect digital files in much the same way that human viruses attack the human body. When a virus infects a machine's files, the virus can spread to other machines when the infected computer sends infected files through the email system or on USB drives.

As one version tells it, the first virus to thwart software piracy came on the scene in 1986. Creators named the virus the "Brain" and infected the boot sector of floppy disks. When the thieves copied the disks, the virus disseminated to their computers.

The main thing to remember about viruses is that they need humans to spread and infect other machines or media.

Worms

Worms operate in a fundamentally different way from viruses. They do not need humans to spread to other machines. Worms infect a computer once. Then they use networks of computers to spread the infection to others, all without the help of human users. Worms exploit weaknesses in email programs and other network and software vulnerabilities. Worms can send thousands of copies of themselves to infect new systems and then the worm's lifecycle begins again.

In the beginning, worms generally disrupted system resources and slowed the infected computer's performance. In today's increasingly digital world, however, worms consist of malicious code designed to steal files or delete them.

Adware

As the name implies, most people recognize adware as the online nuisance that automatically delivers advertisements to computers. Adware includes the ubiquitous "pop-up" ads that disrupt access to webpages as well as ads that come with "free" software.

Adware is mostly a harmless nuisance; however, some adware products contain tracking tools that can steal information from a consumer's browser history as well as the consumer's geographic location and then sends targeted ads to his computer. Most recently, security expert Malwarebytes warned consumers that a new type of adware seeks to disable virus software.

Since users voluntarily install adware, it is not malware (which attacks without permission). Adware is a "potential unwanted program", or PUP.

Spyware

Well-named, spyware does just what it says. Spyware collects data like keystrokes, browser habits, and login information which it then turns over to cyber criminals for their criminal purposes. Spyware also changes security settings on infected computers or interferes with network connections. TechEye warns that newer spyware software may track user behavior across multiple devices without consent.

Ransomware

This malware is more vicious. When ransomware infects a computer, it encrypts the sensitive data it finds (personal documents, photos, financial information) and then demands payment of money in order to effect its release. Businesses or individuals that refuse to pay the ransom, risk data deletion as punishment.

Some ransomware encrypts the data and locks the owner from all access to the computer or network. The ransomware known as CryptoWall caused users to report $18 million in losses in 2015 to the FBI's Internet Crime Complaint Center.

Bots

Bots are malware that hackers program to execute specific operations automatically -- without the user's approval or knowledge -- once they infect the computer. Hackers who can infect multiple computers using the same bot create a "botnet" (from robot network). Hackers can use botnets to remotely manage infected computers. Hackers use botnets to steal sensitive or personal data, spy on activities, disseminate spam, or launch denial of service (DDoS) attacks via their managed networks.

Rootkits

Rootkits allow IT professionals to remotely troubleshoot network issues but they can create problems. By design, rootkits give third parties remote access/control to a computer or a network. Rootkits also actively hide their presence. Once rootkits install on a computer, hackers can gain complete control over the computer and its networks. They can steal data or install malware. The only way to uncover this malicious code is by manually scrutinizing traffic for unusual behavior. Best practices also means regularly patching the operating system and software to ward off potential infections.

Trojan Horses
Trojan Horse malware has been around awhile. Like its namesake, these malware programs hide in plain sight by masking themselves so they appear as authorized files or software. Once installed to a system, Trojans can execute changes to the victim's computer and perform malicious code, all without the knowledge/consent of the user.

Bugs
Bugs in software are programmer errors -- not malware -- that can nevertheless have serious effects on a victim's computer. Typical effects involve freezing, crashing, or slowed performance.

On the other hand, bugs in security software are more lethal. They often provide hackers a pathway to avoid security defenses and infect the computer/network. This is why it's so important to keep up with software patches which address specific programming bugs.

Solution
DeviceGuardian™ is a tool that is easily installed on any existing or new device allowing ABT to securely manage all of your mortgage software, data, and users without driving up operating expenses and without reducing efficiency. DeviceGuardian™ PC and Device Protection makes all of your devices compliant with Consumer Financial Protection Bureau (CFPB) regulations.

About ABT
Access Business Technologies, headquartered in Northern California, was founded in 1999 as a leading provider of hosted, on-demand software for mortgage loan origination, servicing and pipeline management. Access Business Technologies (ABT) provides access to business technologies that empower mortgage professionals to safely perform at the top of their game anytime, anywhere. ABT proactively supports, defends and manages game-changing technologies and processes that help mortgage professionals excel.

We are a certified SSAE 16 Type II cloud solution provider to over 500 mortgage financial institutions. We are partnered with nearly a dozen leading mortgage software vendors. Our partnerships with the best mortgage software in the world integrate our cloud suite of products, to empower your workforce to produce more loans safely anywhere and anytime.

References

1. Kaspersky. *usa.kaspersky.com Retrieved 31 January 2017.*
2. *Bit9 + Carbon Black research document*. www.carbonblack.com *Retrieved 31 January 2017.*
3. *AnomALI. www.anomali.com Retrieved 31 January 2017.*
4. *clearswift*. www.clearswift.com *Retrieved 31 January 2017.*
5. *hackmageddon. www.hackmageddon.com Retrieved 31 January 2017.*
6. *Symantec/threat-report.www.symantec.com Retrieved 31 January 2017.*
7. *Channel_Pronet_Work/article.www.channelpronetwork.com Retrieved 31 January 2017.*
8. *NetIQ_Security Statistics.www.netiq.com. Retrieved 31 January 2017.*