Fall 2016

The Shield

A security newsletter for businesses

In this issue:

From cybercriminal gangs to legal risks — security threats highlighted at conference

Just like other profit-seeking enterprises, cybercriminal organizations are adept at exploiting emerging technology to stay ahead. For instance, criminals are using data analytics to gather information for nefarious purposes, cybersecurity expert Andy Chandler warned the nearly 600 attendees at the U.S. Bank 5th annual information security conference in September.

"The criminal infrastructure is continually evolving and maturing," according to Chandler, Senior Vice President of Dutch information technology security consultancy Fox-IT and one of nine speakers at the Trust in Us event in Minneapolis.

Bots, web-crawling software applications that penetrate internet-based accounts, collect massive volumes of discrete data elements about individuals. By themselves, the data elements don't yield enough clues about people's identity to do much damage. But when assembled through big data analytics, robust identity profiles are created that allow cybercriminals to wreak havoc, Chandler explained.

Criminals gaining greater global traction

The increasing efficiency with which criminals can obtain the data required to defraud companies enables them to abandon their traditional focus on the largest financial institutions and companies in northern Europe and the United States. A heat map of cybercriminal activity over the last year presented the increasingly global extent of criminal reach.

He also believes the "Business Club," the notorious syndicate of cybercriminal gangs that was substantially disrupted two years ago by multiple law enforcement agencies, is back in action. He sees the syndicate's fingerprints, such as the effective use of big data analytics, on the latest round of major cybercrimes.

What makes organizations vulnerable to social engineering-based cyberattacks hasn't changed. In Chandler's estimation, "it's the human tendency to talk and to click." The "talking" can mean casually spreading personal information around the internet that can be drawn into big data warehouses; clicking is what makes people vulnerable to malware.

Continued...

usbank

Embedding malware to attached Word documents emailed to employees of targeted companies has been a successful cybercriminal tactic recently, Chandler noted. Because Word attachments are ubiquitous in corporate networks, employees aren't sufficiently suspicious of them and fall into the trap.

Beyond technological solutions, the best remedy to cybercrime is an ongoing, aggressive effort to educate employees about keeping their guard up, Chandler said.

Legal hazards

Ultimately, organizations want to both prevent successful attacks and minimize legal liability in the event an attack is successful. "Unfortunately, the number of sources of legal risk is multiplying all the time," said another speaker, attorney Harriet Pearson, who chairs the international law firm Hogan Lovells' Cybersecurity Solutions Group.

One hazard is the prospect of lawsuits from customers harmed by a company's inability to deliver a promised service due to a cyberattack. Manufacturers also face similar legal concerns, particularly when their products contain potentially vulnerable electronic components. "The automobile regulators have become extremely active in reviewing manufacturers' cybersecurity posture," Pearson said.

Several federal regulators are pressing companies to have and follow detailed procedures designed to secure data from external and internal threats. "Enforcement activity is picking up," Pearson observed.

Data theft by internal "rogue employees" has become "an exceedingly common event," she added. Legal questions arising from what she calls "bad apple activity," as well as external threats, include:

- What steps were taken to prevent it?
- What steps were taken to detect it? And:
- How was it addressed when discovered?

Ultimately there is no way to guarantee safety from a cyberattack, Pearson said. Thus one of the biggest management challenges is determining what level of investment in cybersecurity measures would be deemed "reasonable" in the event of litigation stemming from a breach.

While there is no clear answer, taking security-enhancing steps after a careful analysis of an organization's particular vulnerabilities is the prudent way to go, she said.

Continued...

About Trust in Us

U.S. Bank held their 5th annual Trust in Us Conference on September 21, 2016. The free, invitation-only conference serves as a forum to hear from world-class experts to explore the complex and evolving cyber risk landscape. In addition to Andy Chandler and Harriet Pearson, participants heard from the following speakers: Jason Witty, U.S. Bank Chief Information Security Officer; Phil Agcaoili, Elavon CISO; Josh Corman, Chief Technology Officer for Sonatype; Michael G. Gelles, Director with Deloitte Consulting, LLP – Federal Practice; Philip Reitinger, President and CEO of the Global Cyber Alliance; Renee Tarun, Deputy Director of NSA Cyber Task Force; Dominic Venturo, Chief Innovation Officer at U.S. Bank; Valerie Abend, Managing Director and Head of the U.S. Cybersecurity Practice; and Keynote Speaker, Amias Gerety, Acting Assistant Secretary for Financial Institutions.

Contact your U.S. Bank representative if you would like more information or are interested in attending future U.S. Bank events.

Andy Chandler, Fox-IT,
at the 2016 Trust in Us conference

Harriet Pearson, Cybersecurity Solutions Group
at the 2016 Trust in Us conference

Jason Witty, U.S. Bank Chief Information
Security Officer, speaks at the 2016
Trust in Us conference

Data breaches: an ongoing problem for businesses

Cybercriminals continue to look for opportunities to steal valuable data day and night. Their sophisticated attacks are specifically designed for widespread deployment. These attacks typically go unnoticed by business owners, detected only when fraud patterns are identified within a particular business segment. For example, recent breaches have involved malware injected into Point-of-Sale (POS) systems.

The ID Theft Resource Center (ITRC) has reported 638 confirmed data breaches since January 2016. According to ITRC reports, 2016 is set to outpace 2015 for the number of confirmed data breaches. The frequency and sophistication of these cyber-attacks against card data continues to be a growing problem for businesses, both big and small.

Business owners that want to protect themselves from the liabilities associated with a data breach should isolate sensitive payment information from their POS, which lessens the opportunity for exposure of the POS in the payment authorization process, thereby reducing the scope of Payment Card Industry Data Security Standard PCI DSS compliance requirements.

A robust approach to security that protects a business and safeguards customer card data includes the following:

- Format Preserving Encryption (FPE) utilizing advanced cryptography, which addresses the challenges associated with securing cardholder data upon initial entry into the payments ecosystem.
- Tokenization that replaces sensitive payment data with alias values or tokens that can be stored in lieu of sensitive card numbers. Tokens can be used for subsequent transactions like adjustments or voids, or may be utilized in the back office for accounting or analytics. Tokens are useless to criminals attempting to steal card data.
- EMV chip card technology authenticates payments to block counterfeit card transactions and can reduce costly card-present fraud related chargebacks.

Simplify® is a U.S. Bank security solution for payment devices that offers businesses the layered security approach necessary to protect sensitive card data from compromise. Through Simplify, businesses benefit from the security technology of encryption, tokenization and EMV, while being able to accept traditional swipe payments, newer EMV chip cards, and the latest in Near Field Communication (NFC) and contactless mobile wallets. Simplify integrates with all major POS providers, such as Oracle MICROS, and can seamlessly work with both current and legacy systems. Also, through Simplify, sensitive cardholder data can be isolated from the payment system. This supports better compliance with card data-related regulations like PCI DSS.

Ask your U.S. Bank relationship manager for more information about the importance of a layered security approach today.

Security best practices for online business banking: SinglePoint® and SinglePoint* Essentials

Security is important when you're managing your organization's finances online. If your business banks with U.S. Bank, you likely use our online business-banking portal SinglePoint® and/or SinglePoint Essentials for cash management and online banking. That's why, to ensure your safety, U.S. Bank uses advanced levels of online security and monitoring technology, and implements strict policies and procedures for handling your information.

In addition to SinglePoint security measures, we recommend you use a layered security strategy to protect your organization from unauthorized access or malicious activity. The following best practices can improve your organization's security when accessing SinglePoint:

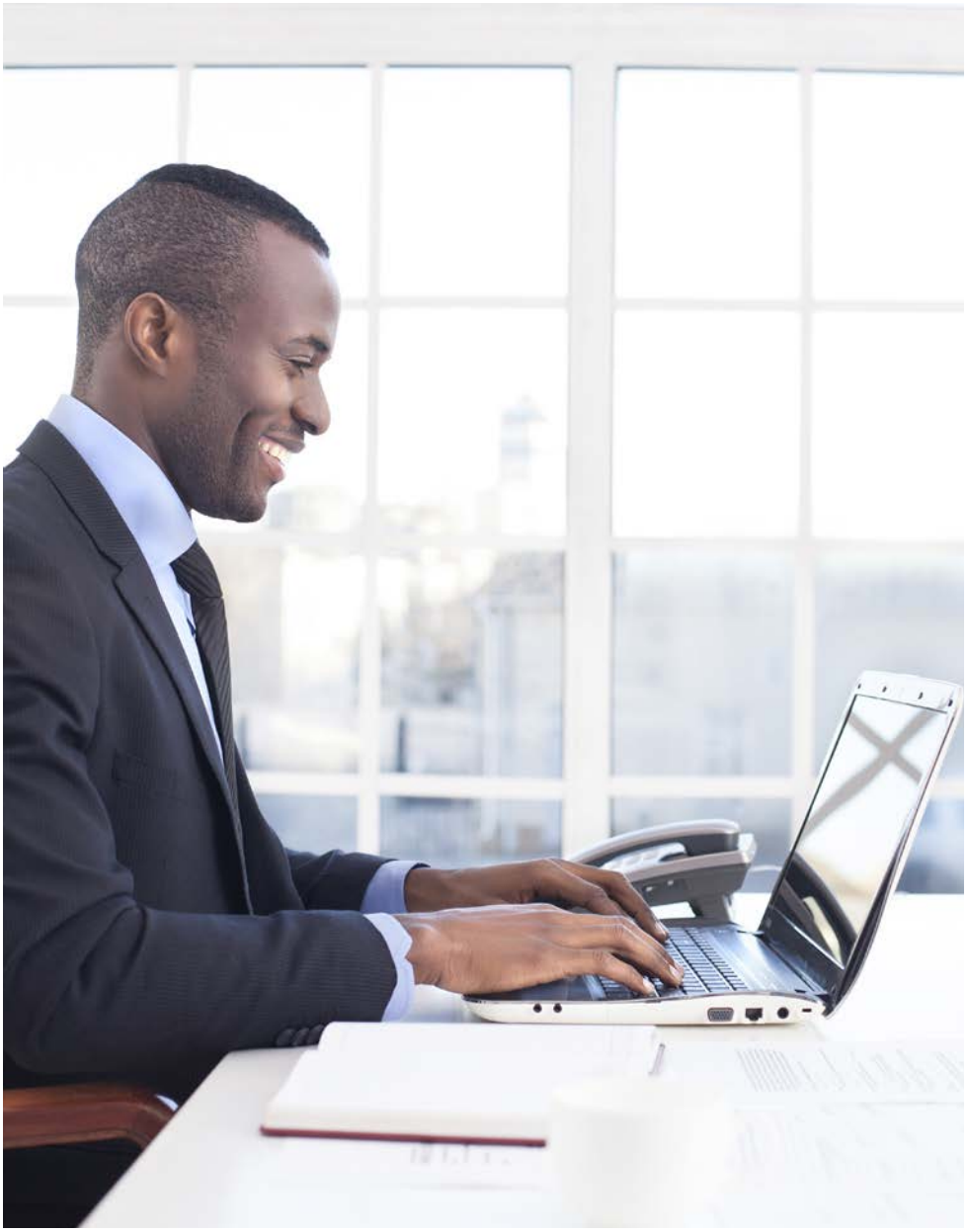
1. Implement dual authorization (including an approver role) for online payments. Dual authorization is one of the stronger defenses against online payment fraud. The FFIEC, FBI, and Secret Service recommend it as a way to combat corporate account takeovers.
2. Have a workstation dedicated only for financial use. Block e-mail and non-financial site access on this workstation to limit opportunities for external network penetration.
3. Stay aware of your account and payment activity. Review the reporting your bank has available to ensure your payments were processed as intended.
4. Use fraud detection and prevention tools. For example, install IBM's Trusteer Rapport for financial malware protection. Trusteer Rapport is available, at no cost, to all U.S Bank clients using SinglePoint. Visit trusteer.com for more information.
5. Limit user access only to those individuals with a genuine business need. Review access periodically and revoke user access for terminated or transferred users.
6. Keep user account information secure. Never share user IDs, passwords or tokens — even within your organization.
7. Follow internet security best practices. Use a security firewall, keep anti-virus and anti-spyware software up to date, and use caution when receiving emails with links or attachments.

Continued...

*U.S. Bank and SinglePoint are registered trademarks of U.S. Bank National Association.

An ever-vigilant attitude is needed to detect and prevent cybercriminal activity when you're using the internet and accessing web-based systems. Early detection and quick action is important to minimize any potential impact. At U.S. Bank, we ask our online system users to be vigilant and to let us know if they discover any malicious activity.

For more information about online security best practices, or if you observe suspicious activity while using a U.S. Bank online system, please contact your U.S. Bank relationship manager or commercial customer service team.



Middle market thought leader podcast features U.S. Bank CISO

Recently, Jason Witty, U.S. Bank Chief Information Security Officer (CISO), met with Jack Sweeney of Middle Market Executive for a special edition podcast titled "Inside the Cyber Threat: Why It's Time to Protect Your Middle Market Business." The interview sheds light on trends and motives in cybercrime and provides some best practices for securing against it and reacting to it.

Witty explains that the internet, through its ability to connect people all over the world, is like a bad neighborhood. Unlike the physical world, there's no concept of distance to separate countries, companies and individuals from the "bad guys." They're literally milliseconds away and their motivations for cybercrime are constantly changing and evolving. "That's why," Witty says, "preventive, detective, responsive and recovery-type security technologies are necessary."

Among other measures, information sharing provides a better understanding of the threat landscape. It helps governments develop applicable laws and regulations, and companies tailor prevention mechanisms and controls.

In addition, it's becoming increasingly important to take a layered approach to security. Witty states, "In information security, you can't just do one thing." He recommends that companies follow a security framework. For example, the National Institute of Standards and Technology (NIST) cybersecurity framework offers a simple, yet robust, approach for analyzing threats, assessing gaps and developing a go-forward strategy.

Witty also warns listeners of two common threats facing companies today. The first is business email compromise. It involves an intricate scam where criminals research individuals in an organization (often through social media sites and social engineering) and impersonate them through email. A common variant of the scam occurs when the criminals draft an email from a high-level executive, like the CEO, and request an immediate transfer of funds for an important, "hush-hush" deal that was just made. Typically, the scam is successful when the transfer is made without performing a call-back to confirm the origin and authenticity of the email. Witty explains that a good defense against business email compromise starts with employee education.

Continued...

The other common threat facing companies, and rising in occurrence, is ransomware. This scheme involves malware that, when deployed, encrypts important data and files in the organization. The bad guys then hold the data "at ransom," requesting payment before unlocking the data. Witty says that in addition to employee education, good backup and recovery controls will help defend against ransomware.

The full podcast is available on middlemarketexecutives.com (middlemarketexecutive.com/data-security-jason-witty-usbank/).