Cybersecurity:
Managing Risks to Credit Cards

Cybersecurity represents a top concern for the financial services industry, recently dominating headlines with a high-profile September 2017 breach, in which criminals hacked the personal information of over 140 million Americans. Credit unions must prepare to meet ever-evolving cyber threats and quickly prevent, detect, and mitigate these risks, even as they become more sophisticated and frequent. Credit unions may decide to counter these trends on their own or with a trusted partner, but either option must deliver peace of mind through a layered and comprehensive approach.

The Threat Horizon – Leading Cybercrimes

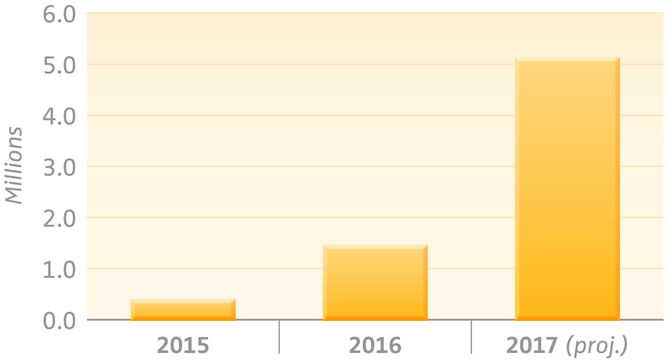
Ransomware

Ransomware is the fastest growing cyber threat, targeting users of all types—from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300 percent increase over approximately 1,000 attacks per day in 2015. Attacks in 2017 are projected to rise 250 percent and total costs to exceed $5 billion with roughly a quarter of this total in the United States.[1]

Ransomware will hold a credit union's data hostage until a payment triggers a release of control. Ransomware allows cyber criminals to realize a fast reward, usually a small sum, and then move on quickly to the next target. Ransomware sneaks onto systems using email attachments and embedded hyperlinks within emails, exploiting internet or web application vulnerabilities. It is easy for an employee to accidentally click on a file. Once installed, the malware encrypts files, drives, and locks down the system. The hackers then send messages demanding money to decrypt the files. Tracking this criminal activity becomes more challenging as the requested payment often takes the form of Bitcoin, limiting the ability to trace the payment.

Ransomware Attacks 2015–2017

Source: www.us-cert.gov



Phishing and Business Email Compromise

In May 2017, the FBI reported that more than $5 billion had been lost to business email compromises, including phishing.[2] Phishing attacks occur when a criminal poses as a trustworthy source to obtain information or funds. Often a criminal will pose as a CEO or company employee and request funds or confidential information. Credit unions risk monetary losses and compromising member information if they fail to recognize these attacks.

According to Robert Steadman, Vice President, Security and Compliance Consulting at Herjavec Group, "Each day around the world, 294 billion emails are sent and it is estimated that more than 90 percent of them are spam. Of the reported 37.3 million instances of phishing attacks, 88 percent involved users clicking a link. Social engineering has proven itself to be an effective means by which threat actor groups can exploit human cognitive biases to gain access to sensitive information and assets."[3] The diagram on the next page lays out this common pattern. The most effective way to fight phishing includes employee training and awareness.

[1] Anthony Cuthbertson (2017, May 23). Ransomware Attacks Rise 250 Percent in 2017, Hitting U.S. Hardest. Newsweek. Retrieved August 29, 2017 from http://www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034

[2] Business E-mail Compromise E-mail Account Compromise The 5 Billion Dollar Scam (2017, May 4). FBI Public Service Announcement. Retrieved September 12, 2017 from https://www.ic3.gov/media/2017/170504.aspx

[3] Morgan, Steve (2016, August 17). Hackerpocalypse: A Cybercrime Revelation. Retrieved August 24, 2017 from https://www.herjavecgroup.com/hackerpocalypse-cybercrime-report/

Phishing Threat Diagram

Source: Jenny Menna, Elan Financial Services

SEND
Account Name
AlexMartin@email.com
Password
●●●●●●●●

Phishing Email	Bait Taken	Credentials Stolen
A fraudulent email is sent masquerading as legitimate.	Phisher tries to acquire victim's login credentials or account information.	If successful, the phisher can use login credentials or account information for their purposes.

How Do Cybersecurity Threats Impact Credit Card Issuers and Cardmembers?

Data breaches, point-of-sale attacks, the creation of sophisticated new forms of malware, and the introduction of "cybercrime-as-a-service" are now key issues affecting the security of credit card data.[4] Despite the implementation of EMV technology, credit and debit card fraud alerts are up 15 percent from two years ago, according to a CreditCards.com survey report. Thirty-one percent of U.S. adults have received a fraud alert regarding a credit card.[5]

Criminal fraud techniques on credit cards evolve quickly. Instead of selling just hacked card numbers, thieves will sell accompanying information, such as zip codes, used to authenticate transactions.

When making purchases, criminals will attempt to swipe a dummy EMV chip card and provide information to validate a stolen identity, after claiming the chip is defective. This negates security benefits of the EMV chip.

While criminals have found a way around using the EMV chip, card issuers have been assuming the burden of risk associated with criminal activity. Some merchants have prolonged deadlines for EMV adoption. By 2020, card issuers will no longer be allowed to charge back non-EMV merchants for purchases under $25 and will only be allowed to charge back ten fraudulent transactions per account. These regulations delay the full benefit a card issuer may have expected from EMV adoption.

Armed with the latest cyber threat information and statistics, how can credit unions monitor, predict, reduce, and manage the risk?

According to Jenny Menna, Elan Financial Service's Security Intelligence, Engagement & Awareness, Cybersecurity Partnership Executive, the first line of defense is instituting measures designed to anticipate emerging threats and risks. These measures enable business growth while protecting existing revenue and safeguarding

[4] Galvan, Suzanne (2017). New Tools For Combating Data Breaches And Safeguarding Consumer Card Payments. Retrieved August 23, 2017, from https://finance-technology.cfotechoutlook.com/cxoinsights/new-tools-for-combating-data-breaches-and-safeguarding-consumer-card-payments-nid-146.html

[5] Strozniak, Peter (2017, May 12). Credit/Debit Card Fraudsters Target the Affluent. Retrieved July 5, 2017, from http://www.cutimes.com/2017/05/12/credit-debit-card-fraudsters-target-the-affluent

against attacks.[6] Cyber strategies also must be comprehensive and layered:

- They must be intelligence driven.
- The right tools, products, and partners are critical.
- As the number of exposed risk points increases, cooperation, integration, and partnership across stakeholders is critical to anticipating the next attacks.
- They must involve the nine ecosystem components: data and information, networks, devices, applications, identity and access, third parties and vendors, industry and partnerships, customers and clients, and employees.

Failure to address cyber threats effectively may harm a credit union's core business.

What Does The Future Hold?

The "internet of things" represents the increasing network of devices that connect to the internet. Connected devices offer personalized customer experiences but also increase the number of potential access points to confidential information. With each digital tool that credit unions offer their members, new vulnerabilities will likely follow. To address the changing threat environment, credit unions need to take a broader, intelligence-based approach to cybersecurity, factoring in new threats such as the geopolitical climate, third-party risk, and exposed insiders.[7]

A focus on security may soon become table stakes in the pursuit and engagement of members. Eight out of ten respondents to a May 2017 survey want biometric authentication beyond the fingerprint in their mobile banking and payment apps and 42 percent said they refuse to use mobile banking or payment apps that do not have biometric authentication.[8]

The right credit card partners will help manage risks and drive profitability, while fostering resilience to attacks through people, processes, and products.

Choosing a reliable payments partner with leading-edge technology may help mitigate the threat to credit card issuers and cardmembers. Outsourcing credit cards to a trusted partner, such as Elan Financial Services, offers credit unions the opportunity to increase operating efficiencies, introduce economies of scale, and streamline processes. Elan continues to aggressively invest in its agent financial institution program, making cybersecurity improvements to benefit both existing cardmembers and Elan's nearly 1,400 active financial institution payments partners.

Geolocation Adds a New Layer of Protection

Elan offers a comprehensive suite of card fraud protection products and has increased access to digital innovations, including text alert capabilities, a Geolocation Service App, and fingerprint authentication for mobile applications. Elan's geolocation technology integrates into the issuer's mobile credit card app and enables the location of a card transaction to be matched to the location of the user's phone. By matching the two, the issuer has more data about the transactions to use in

[6] Menna, Jenny (2017, February 7). Keeping your business safe in a risky cyber world. ASLRRA Connection Magazine.

[7] Geyres, Stéphane and Orozco,Michael. (2016, April). Think banking cybersecurity is just a technology issue? Think again. Accenture Strategy. Retrieved July 24, 2017, from https://www.accenture.com/us-en/insight-think-banking-cybersecurity-technology-issue

[8] Orem, Tina (2017, May 4). Many Consumers Avoid Banking Apps Without Biometrics: Study. Retrieved July 7, 2017, from http://www.cutimes.com/2017/05/04/many-consumers-avoid-banking-apps-without-biometri

making approval decisions when cardmembers make out-of-pattern purchases. Enabling geolocation both domestically and internationally can help avoid disruption to cardmembers, easing their travel challenges and concerns about fraudulent point-of-sale purchases.[9] In particular, this technology can help reduce the occurrences of ''false positives,'' a decline at the point-of-sale based on an unexpected transaction. These false positives are one of the most challenging issues travelers experience when using credit cards.[10]

From activation strategies and card level verification checks to real-time card blocking and safer online payment options, our solutions and fraud experts provide layers of security—allowing your cardmembers to use their cards with greater confidence. The Elan detection system further overlays the authorization process and triggers any abnormal spending habits, allowing our partners and their cardmembers to feel confident that their card is secure.

About Elan Financial Services

For almost 50 years, Elan has delivered best-in-class credit card products and service to its valued financial institution partners. Today, Elan helps nearly 1,400 financial institutions manage the changing fraud landscape, using the strategies mentioned above, along with many other industry-leading trends. Year after year, our partners remain pleased with the Elan solution, as Elan has seen a more than 95 percent renewal rate.

For more information, visit cupartnership.com.

Elan™
CREDIT CARD

[9] Mobile Location Confirmation. (n.d.). Retrieved January 27, 2017, from https://developer.visa.com/products/mlc

[10] Geolocation Technology: Adding Security and Reliability to Credit Cards (2017, April). Retrieved October 4, 2017, from https://www.cupartnership.com/resource-library.html