The Key to Credit Union Resilience
Page 3

The Dark Web Has a Silver Lining
Page 6

Do you really know who your members are?
Page 10

Hitting the Jackpot
Page 12

How to Prevent Cyberattacks
Page 14
Save the dates... April 14-17, 2019

NACUSO

2019 NETWORK CONFERENCE
at the Grand Hyatt San Diego

NACUSO Partners

Exclusive Premier Card Partner

mastercard.

Platinum Partners

cu Revest
CU Answers
CUNA Mutual Group
CUSO Financial Services LP
PSCU
CO-OP Financial Services

trellance
CU Lending Cooperative
CUProdigy
CU Direct

Gold Partners

Open Technology Solutions
CC
Credit Union Student Choice
Midwest
ALKAMI
Gateway
CloudCherry
buzz
Ongoing Operations
FICO
The Key to Credit Union Resilience
By Gene Fredriksen,
Chief Information Security Strategist at PSCU

A cyber security function for any organization is made up of the proper combination of People, Process and Technology. The three must work in concert to mitigate organizational risks and ultimately protect the information entrusted to us. Achieving that balance is not easy, but it is critical to the success of the organization as it impacts financial planning and product direction. We must not only understand the business needs and environment of the organization, but also the emerging threats facing the industry.

As the credit union industry matures, regulators like the National Credit Union Administration (NCUA) are coming to the realization that just being safe is not enough to serve members. A couple of years ago, the Department of Homeland Security introduced the concept of resilience. In plain English, resilience can be defined as the ability of a business to not just survive but also to thrive in a rapidly changing or potentially caustic environment. It describes the state of an operation wherein members have secure access to the right data, delivered to the right place, when the member needs it. It encompasses much more than the traditional view of cyber security.

The speed of new threats is increasing, and the potential impact of a single piece of malware continues to grow, which is why the NCUA and other regulators are focusing on the concept of resilience. As the pace of threats moves more quickly and members expect more from our digital tools, security technology must be agile, not static as in the past. The security systems of today must be highly available, agile and quickly deliverable, which requires a balanced approach of People, Process and Technology controls, tied to and commensurate with business risk. A robust process that adjusts controls as business risk changes will help establish a strong defense program for an organization. When the program is constantly evaluated against business risk and emerging technical threats, the program will remain strong. As always, there are no guarantees against a breach, but the best defense is a strategic, balanced program.

“As an industry, we have chosen to pursue an e-business and mobile strategy. In a highly competitive e-business environment, resilience is key.”
This is all well and good in theory. But when funding and headcount is at a premium, what are the ways an organization can positively affect the People, Processes and Technologies in place to support the protection programs?

**People:**
Continually train all employees through:
- Electronic learning
- Instructor-led training
- Department meetings
- Email security reminders

The watchword for the People area is “culture.” When people know what to do and they view it as their personal responsibility, a culture of security is taking root. Just as with any training, continual messaging and reinforcement is critical.

**Process:**
Continually enhance security to address evolving threats.
- Security should be designed with a focus on segregation of duties across all critical areas not just to thwart fraud but also to help prevent accidental damage or destruction of information assets.
- Focus on processes to implement critical security patches and updates to make systems more resistant to compromise. Patches and updates are a fact of life. Missing an update can open the door to a hacker, which is exactly what happened in the case of the Equifax breach.

**Technology:**
Many security product vendors would have you believe technology can keep you safe. Every time a new threat or vulnerability emerges, new products also emerge targeted at mitigating the risk. Implement security technology to facilitate the enforcement of required security protocols.
- Select tools that fit into the security architecture, avoiding standalone systems and point solutions wherever possible.
- Leverage security data to identify risks.
- Recognize active threats using data and analytical information.

It takes an organization leveraging all three areas of People, Process and Technology to achieve resilience while improving operational capabilities.
As an industry, we have chosen to pursue an e-business and mobile strategy. In a highly competitive e-business environment, resilience is key. These new tools allow our members to access their information 24 hours a day, even in times of natural disasters. It takes an organization leveraging all three areas of People, Process and Technology to achieve resilience while improving operational capabilities. Well-designed, resilient solutions will also reduce daily “noise” for the operations team, allowing it to focus on infrastructure enhancements to improve uptime and resilience.

The credit union culture is built on member service excellence that differentiates us in the financial services sector. Internally, the focus on resilience will drive greater member satisfaction and trust. Externally, successes in this area will result in greater public trust and give us the opportunity to grow our organizations. PSCU's highly available and secure processes are built to enable the success of credit union resiliency efforts for nearly 900 Owner credit unions. This partnership is not just good for individual credit unions; it is critical to the success of the credit union industry as a whole.

About the Author:

Gene Fredriksen is responsible for several strategic functions primarily focused on relating PSCU’s perspective and stance on cyber security to existing clients, prospective clients, consultants and the industry as a whole. Gene has over 25 years of information technology experience, with the past 20 focused specifically in the area of information security. He joined PSCU in 2013. Since then, he has grown the Information Security and Compliance teams and service offerings, implemented advanced tools and processes, and advanced PSCU's relationship with numerous partners. Gene has served on the R&D committee for the Financial Services Sector Steering Committee of the Department of Homeland Security and is a Distinguished Fellow for the Global Institute for Cybersecurity + Research, headquartered at the Kennedy Space Center. He is also the Executive Director for the National Credit Union Information Sharing and Analysis Organization.
The dark web has been in existence since the 1990’s but has become a household word lately through ads from identity protection companies that offer to monitor the dark web. The ads warn a subscription-paying customer if their data may have been compromised and put up for sale.

The dark web is where fraudsters conveniently sell breached data such as usernames and passwords, credit and debit card data, alongside complete identities, passports, drugs, guns, and worse. The dark web, and the crimes associated with it, is a big and sophisticated business. There are fraudsters that specialize in obtaining the data. There are other fraudsters that specialize in validating the data, using bots to try the usernames and passwords on hundreds of sites, and others that specialize in testing the credit and debit card numbers on unsuspecting ecommerce merchant sites. Downstream, other fraudsters take the useable payment credentials and either create counterfeit cards or launder the card numbers by buying electronics and gift cards through online merchant sites. Still others use the validated usernames and passwords for account takeover fraud, draining bank accounts. These groups buy and sell their data on the dark web, creating an entire economy of fraud, and its thriving. Fraudsters go where the money is. But a new business is also thriving from the same economy – the many services that claim to monitor the dark web on behalf of concerned clients. This is starting to shed light on the dark web, and that is unwanted by the bad guys.

What is the dark web?

To understand how these two business models are at odds, it’s necessary to first understand what is the dark web. It is not a separate network, and it was created by the U.S. government for intelligence operatives (i.e. spies) to anonymously exchange information over the world-wide-web. Just like Napster and Aimster worked over the web to exchange music anonymously by downloading proprietary software for music and movie files to be exchanged, the dark web also requires special software. The software is called Tor and it allows you to navigate websites that are proprietary to the dark web.

While theoretically anyone can download Tor and start browsing, law enforcement, internet service providers, and the bad guys are all tracking computers that access the dark web. Federal and international security agencies are looking to track activity, while the bad guys will test each new computer that accesses the dark web to see if they can gain access to the camera and laptop, as well as the O/S to install malware. This threat is usually enough of a deterrent that only fraudsters, and security specialists are the ones accessing the content on the dark web. That content is usually in the form of a marketplace, like eBay, with some becoming familiar names, such as Alphabay, Silk Road, Crypto Market, and Hansa. According to the FBI,
Silk Road made a total of $1.2 billion between 2011 and 2013 when it was shutdown (although Silk Road later re-emerged). Prices are always posted and transactions are usually conducted in Bitcoin, with some marketplaces accepting other cryptocurrencies. And in an ironic twist, marketplaces allow buyers to post ratings of sellers to weed out the bad sellers from the good ones.

A screenshot from a session provided by Executive Security Advisor of IBM Security, Etay Maor shows one site’s homepage where buyers can choose from “products” ranging from jewels, credit and debit card numbers, gold, drugs, malware and ransomware software, and weapons, as well as services such as stolen credit card laundering, skimming placement and retrieval, and even bomb threat services where the seller will call a school and make a threat in order to get a student out of taking a test.

The marketplace on the dark web constitute big business, with combined daily volumes that reach $650,000 at peak (averaged over 30-day windows), while researchers say the total is generally stable between $300,000 and $500,000 a day.

The companies that monitor the dark web also constitute big business, with examples like Terbium Labs raising $6.4 million in venture capital funding, and Cybersecurity firm FireEye acquiring threat intelligence company iSight Partners for $200 million.

If the dark web is being monitored by good guys, why is it still in business?

The dark web is surprisingly transparent – it’s open to anyone to access, to buy and sell goods and services, and is very efficient at connecting buyers and sellers, albeit for illegal and illicit purchases. If monitoring companies and law enforcement have such easy and open access to this activity, why does it still exist? Three primary reasons: money, anonymity, and a high level of sophistication. The amount of money being transferred over the marketplaces on the dark web dwarf the GDP of most nations, and as long as buyers and sellers can conduct their transactions in the open, but remain completely anonymous and untraceable, then these transactions will continue, and these marketplaces will continue to grow. In an example of how sophisticated these marketplaces are, according to Krebs on Security, one cybercrime marketplace’s own security system triggered a “pig alert” and brazenly flagged the fed’s transactions as an undercover purchase placed by a law enforcement officer.

There is also a timing element to the monitoring activity. In the case of a credit card breach, by the time a monitoring company finds a new batch (or “dump” as they are referred to on the marketplaces) of card numbers for sale, those cards may have already been stolen, possibly counterfeited and laundered. Unlike physical goods, a batch of stolen card numbers can be sold several times.

How can CU’s make member card data less valuable on the dark web?

As long as there is a mag stripe on credit and debit cards, and as long as merchants allow a 16 digit number to be used to make a purchase, there will be card breaches, counterfeit cards, and online card fraud. But
there are some definitive steps that credit unions must take to make their members’ data less valuable on the dark web.

1. Enable EMV and reissue chip cards. The level of sophistication of the fraudsters should never be underestimated. The bad guys are tracking which BINs have not been enabled for EMV. Those BINS are specifically listed on the marketplace as readily counterfeit-able, and draw a bigger price tag.

2. Tokenize BINs and encourage members to use Visa Checkout, MasterPass, or Apple/Samsung/Android Pay when making purchases online.

3. Monitor for patterns and be quick to act. Be on the lookout for authorizations with no settlement – that’s a sure sign that bad guys are testing out counterfeit cards before making bigger purchases. Identify enumeration testing, where fraudsters are looking for a good account number, expiration date and cvv2 values.

4. As soon as CAMS and ADC alerts are issued by the networks, be quick to shutdown identified cards and notify the cardholders.

5. Educate members, continuously, on best practices, such as using credit instead of debit, turning on email and text purchase notifications, and never clicking on links in emails or websites unless they can be completely trusted.

None of these steps by themselves will keep fraud from occurring 100%. However, with a comprehensive fraud management and prevention plan in place, a credit union can help make their member’s data unusable by the bad guys.

About the Author:

Lou Grilli is the director of Payments Strategy at Trellance and is responsible for providing leadership to the organization for emerging payments and industry trends, as well as managing the product portfolio. Prior to joining Trellance, Lou was director of mobile products within the North American Retail Payments division at FIS. There, he was responsible for enabling seamless access from smartphones and tablets to FIS products and services. Lou holds an MBA from Duke and a master’s degree in computer engineering from the University of South Florida.
Cracking the Mobile Biometric Conundrum: Assess, Educate and Deploy

The demand for mobile biometric technologies is undeniable

Consumers are excited and looking to adopt...

93% prefer biometrics to passwords

And banks are equally enthusiastic

92% want to adopt biometric technology

Yet knowledge gaps are slowing adoption

36% of decision makers involved in implementing mobile biometrics say they have adequate experience

Getting Mobile Biometrics Right

Mastercard and the University of Oxford have developed The Five Factor Framework to help banks understand and successfully deploy mobile biometrics.
In the credit union industry, knowing who you are talking to is fundamental to having a relationship with your member.

Do you really know who your members are?
By Rick Cranston, Chief Operations Officer for CULedger

To that end, there is a major shift occurring in the credit union marketplace. No longer is it “good enough” for a credit union or a financial institution to validate the identity of a member through two factor authentication or multi-factor authentication. Can you really trust that MFA works every time? It’s equally important today for a member to know who they are speaking with. Both are now required for a real relationship to work. That notion of knowing who you are talking to with context, both as a member and a credit union is foundational to the credit union industry. Literally every interaction between a credit union and a member starts only when we have answered the fundamental question of who you are talking with. CULedger has identified self-sovereign identity as the answer both today in the future.

Digital identity is one of the oldest and hardest problems to solve on the Internet. There is still no way to use digital credentials to prove our online identity the same way we do in the offline world. Distributed Ledger Technology is providing a path to that end. Important changes are happening. First, the World Wide Web Consortium (W3C) is standardizing the format of digitally-signed credentials. Secondly, the technology allows for the provision of decentralized registration and discovery of the encrypted data needed to verify digital signatures. These two steps pave the way for self-sovereign identity—lifetime portable digital identity that does not depend on any central authority and can never be taken away. MyCUID, developed in coordination with Sovrin, Best Innovation Group, and Evernym is being designed exclusively for this purpose, including consideration for governance, scalability, and accessibility (minimal cost and maximum availability).

A physical credential is relatively easy to verify: a human makes a judgment about a paper document. We do it every time we fly, use our driver’s license, our social security number or our library card. Hotel clerks, car rental agents, librarians, and security guards all know the basic procedures for verifying a physical credential from your wallet, except, as we now
Do you really know who your members are?

know, there are significant varying degrees of certainty.

There is the bad news of course. It seems that this same process is not easy to duplicate online. To begin with, on the other end of an Internet connection, you don't have a human—you have a machine. And the credential you are showing them is not a physical document they can inspect, but a digital document. So now what?

To verify a digital credential, we need to solve two problems. First, we need to standardize the format of a digital ID by working with groups of people and organizations, in our case, CU’s, to discuss and agree on what that standardization is and how it works. That’s the “MyCUID Framework for Trust”. Because a digital credential is read by a machine, it needs to be in a format that computers can understand. We’re already seeing this today with some paper credentials that must be verified all around the world, such as passports. Even though it is a physical document, a passport includes sections that are machine-readable in a standardized format.

Second, we need a standard way to verify the source and integrity of these digital credentials. MyCUID solves both problems.

MyCUID, powered by CULedger and its world class partnerships are designing the world’s first industry wide network that first starts in knowing who you are talking with and secondly, integrates the same world class credit union solutions that our industry uses today.

The digital world is changing faster than ever and CULedger development of MyCUID is helping to chart a new course for the future.

About the Author:

Rick Cranston is the Chief Operations Officer for the newly formed CUSO CULedger. Prior to joining CULedger Rick served as VP innovation and Product Development for Credit Union Strategic Partners where his focus was on the continued need to innovate on the financial services on behalf of the credit union industry. This is what lead them to Distributed Ledger Technology and MyCUID. Rick was all the Senior Director, Business and Product Development for the Mountain West Credit Union Association for 8 years.
I hit the jackpot!

These are typically words used to convey excitement on the casino floor as the slot machine lights up and a crowd begins to gather to catch a glimpse of the lucky winner. But unfortunately, there is another less altruistic type of jackpot now being pursued. For these winners, there are no flashing lights, no celebratory bells and whistles, no rowdy celebrations in front of the winning machine. It is called ATM jackpottting, and the only people celebrating are criminals.

ATM jackpottting is essentially what the name implies: it involves fraudsters figuring out a way to make an ATM dispense cash by emptying all the cash out of the machine. It is very different than typical ATM fraud whereby criminals steal card information and withdraw cash from a particular account. Worldwide estimates vary, but the total cost of jackpottting fraud is in the multi-million-dollar range. In the U.S. alone, the impact is already in excess of more than $1 million according to the United States Secret Service.

At a high level, there are two ways for criminals to hit the jackpot with ATMs using malware. The first method is to distribute malware from a remote location, execute the program, put the ATM out of service, and have an accomplice go to the machine and take the money. After the ATM is drained, the malware is removed from the machine entirely, making it difficult to ascertain what happened.

This was the method used in Taiwan in July 2016 when fraudsters gained access to a network and were able to steal $2.7 million in cash at 41 different ATMs. This particular incident started with a phishing attack in Europe that allowed criminals to gain network access prior to installing the malware in Taiwan.

The second method is to exploit vulnerabilities directly at the ATM location as was the case with the recent U.S. jackpottting incident in Connecticut. In this scenario, the fraudster gains access to the ATM through a master key or by drilling a hole in the machine to access the ATM's computer. In the latter scenario, a smartphone is then connected to an endoscope to determine where to connect and install the malware. From there, the perpetrator takes control of the ATM and dispenses the cash. Fraudsters have also discovered other areas within certain ATMs to which they can connect besides an obvious keyboard attachment giving them access to the computer. This is usually seen with older off-premise ATMs with easy access where the fraudsters can dress up as an ATM technician without attracting attention.

While the warnings are now out in the U.S., we have not seen a massive jackpottting increase for several reasons. First, IT network security practices are typically more robust at the infrastructure level in this...
country than some areas of the world. Second, ATMs deployed in the U.S. are generally newer and have more current security releases installed. After ATMs are replaced, they are typically placed on the resell market and re-deployed in other regions of the world. These models have older operating systems, out of date hardware and firmware revisions and are usually not properly configured for security, making jackpotting much easier on resold machines.

While large scale jackpotting attacks have not yet been prevalent in the U.S. for these reasons, fraudsters are constantly looking for new ways to find the weakest link. With the declining trend in counterfeit card-present fraud, driven primarily by EMV chip card deployment, other opportunities like vulnerable ATMs are becoming much more appealing.

It is important for all credit unions to be prepared now that ATM jackpotting has been reported in the U.S. Here are three steps credit unions can take to help guard against this type of attack:

1) Continue to focus on keeping networks up-to-date with the latest security and monitoring in order to keep the malware from reaching the ATM from a network perspective. Technology is only one leg on the stool. Review of security processes and staff training are also important components in any plan to protect your ATM fleet.

2) Review your current ATM fleet with a focus on the off-premise deployments where ATMs are not located in the more secure confines of a branch, or where there is easy access to the inside of the ATM through the front panel. In addition to ensuring ATMs have the latest software and firmware revisions, review the security software configuration to ensure best practices are installed and enabled. Windows XP is particularly vulnerable to this type of malware attack. Right now, reports indicate fraudsters are targeting Opteva 500 and 700 Diebold Nixdorf ATMs using a variant of Plotus.D Malware. This does not mean you should rest easy if you do not have these ATMs in your fleet. Regardless of the ATM provider or model, ensure all machines are all running on the latest software and firmware revisions. Ideally, all ATMs should be upgraded to Windows 7 and outdated machines should be replaced entirely.

3) Review ATM location security and processes. How easily can the ATMs be accessed? Many times, fraudsters are able to disguise themselves as service technicians without being noticed by anyone at off-premise locations. Look for ways to make it more difficult to access ATMs where possible. Ensure you have separate security cameras monitoring the ATM that are not connected directly to the ATM or kiosk.

ATM jackpotting is another variant of a long list of tactics used to commit financial crimes that has reached the shores of the U.S. Create a proactive plan now to address it. Network, ATM and location security updates are the best weapons to prevent your ATMs from becoming part of fraudsters' favorite casino.

About the Author:

Jack Lynch leads PSCU’s Fraud and Risk Management Operations area. Jack has over 25 years of leadership experience delivering operational services, project management, client implementations, process re-engineering, account management, training and technology services.
Cybercrime has spread like wildfire across the consumer landscape. According to Accenture, cybercrime incidents went up 27 percent in 2017. And, costs to combat cybercrime are skyrocketed as well – up 23 percent over 2016 levels.

As alarming as these statistics are, there are measures your credit union can take to strengthen security across systems and data – this year and beyond.

Focus on Fundamentals

“The biggest issue, hands-down, is distraction,” said Paul Love, Chief Information Security Officer for CO-OP Financial Services. “With so many shiny new cybersecurity ‘toys’ on the market, security teams can get distracted from deploying the basics of information security.”

According to Love, credit unions need to ensure that their cybersecurity experts very selectively implement disparate tools that address of-the-moment threats. “That’s not to say that some of these one-off solutions don’t have a place,” he said. “Many of them are incredibly well built and do an outstanding job of protecting against the threat for which they were designed. But, what happens, especially for small and even mid-sized organizations, is that the security lead gets pulled in too many directions.”

Complicating matters, he adds, is the reality that many of the disparate tools being offered as solutions are difficult to “plug in” to the credit union enterprise. “It can take a lot of work to integrate and train staff on new software,” said Love. “My advice to security teams, particularly those with limited resources, is to focus on the basics.”

Keep Systems Patched

Love’s number one cybersecurity best practice for credit unions is to make sure systems are patched, and that analysts are getting the necessary alerts from vendors and associations to understand when and how to patch systems.

“Get your firm locked down with some rock-solid identity and access management systems, policies and procedures,” he said. “Make sure passwords are changed on a regular basis as well. These are not the trendy, rock-star initiatives that will blow up your LinkedIn profile, but they are the ones that will keep your credit union the safest.”
Create a Cybersecurity Champion

Love also advises credit unions to place a single employee in charge of information security. "If this task ends up being someone’s secondary job, that employee’s primary job will take precedence, and this is not a good practice," he said.

He also points to the importance of maintaining consistent policies and standards.

"Applying security consistently across the organization sets the baseline for what the credit union expects from its employees," he said. "Breaches most often occur out of simple carelessness – for example, when an employee clicks on a phishing e-mail."

Address Breaches Immediately

To mitigate damages should a breach occur, credit unions should have a formal incident response program in place.

"When a breach is discovered, credit unions need to react quickly, both containing the damages and communicating well with members and the community," he said. "If you leave your member base speculating on the situation, trust will erode."

He continued, "Fraud evolves and advances rapidly. Investing in security infrastructure, including neural networks and machine learning fraud detection tools, is critically important. But it is also important to teach members how to be responsible with cards and accounts."

To that end, Love recommends making security tips available to members in the branch and on the credit union website. He also advises credit unions to encourage members to freeze their credit, subscribe to a third-party monitoring solution, and download a mobile security app for card controls and alerts.

"Involving members in the fight inspires their loyalty and shows them that you are watching out for them," he said.

About the Author:

Bill Prichard is Director, Public Relations, for CO-OP Financial Services, based in Rancho Cucamonga, California (www.co-opfs.org), a provider of payments and financial technology to credit unions.