4 EFFECTIVE STRATEGIES CISOS CAN TAKE TO BUILD A RESILIENT PAYMENTS FUTURE

Julien Bonnay and Bryce VanDiver

Digital payments crime is increasing. COVID-19 is accelerating payments attacks against financial institutions (FIs), consumers, and even companies as the pandemic changes buying habits to online purchases with contactless payments and promotes a shift to remote work.

Is there a path towards disinfecting digital payments despite these current trends? We believe there is. By strengthening security around digital payments, hardening defenses in the cloud, and encouraging consumer-education campaigns, we see the foundation of cyber hygiene steps for building a resilient payments future.

Here are four actionable recommendations for FIs to follow beyond increasing the basic rules of cyber hygiene.

1. USE INTELLIGENCE TO ANTICIPATE THREATS AND MITIGATE OR LIMIT A LOSS

In erecting barriers to the most sophisticated or powerful cybercriminals, especially those related to state-sponsored actions or B2B scams, the best mitigation is usually intelligence. Knowing who your adversary is, their likely attack methods, and their motivations serve as the base for a threat intelligence-driven strategy.

There is a robust market for cyber threat intelligence, so it is widely available to payment processors and card providers. The difficulty for the FI is not intelligence, but rather the time to analyze the data and apply it to the individual organization's threats. This intelligence is often unused, cast off to a deep corner of a remote data warehouse.

We believe FIs would be well served to build a capability around what is commonly called a Cyber Fusion Center (CFC). The CFC is the next generation of the Security Operations Center (SOC), which organizations have depended on historically to detect attacks and contain the damage. By contrast, the CFC extends well beyond this classic "moat and castle" defense.

2. REDUCE THE ATTACK SURFACE INTERNALLY AND IN THE CLOUD

The boom in Internet-exposed assets from years of digital transformation, and accelerated by a seismic shift to a remote workforce in response to COVID-19 can make protecting your FI's digital attack surface feel overwhelming. FIs are responsible for defending their internal network and their digital presence across the internet and the cloud.

Bringing the enormous scope of an organization's attack surface into focus helps frame the challenges of extending cybersecurity outside the corporate firewall, especially as staff forced to work from home push that boundary farther out. One way to do it, is to red team the cloud and other pathways and blind spots that hackers exploit.

Red teams are a favorite tool of the military, and their task is simple: find flaws in the organization that can be exploited by the enemy. Red teamers, who report to and are supported by top commanders, are granted much leeway to act like insurgents and reveal vulnerabilities invisible to the rest of the organization. We think every medium- and large-scale organization should create a red team to attack itself using a three-tiered attack-and-discovery

approach of 'outsider with no knowledge,' 'outsider with limited knowledge,' and 'an insider with knowledge' to provide a real-life test of their exposure to known security vulnerabilities.

3. AT THE POINT OF SALE, INCENTIVIZE THE USE OF CHIP AND PIN READERS AND TOKENIZATION

Two technologies can lead the defense at POS transactions: Chip & PIN and tokenization. Unfortunately, too many merchants still accept cards with user information embedded on magnetic stripes in the U.S., a technology from the 1960s. As a secondary check, retailers ask for the user's signature, scrawls that are rarely challenged. These technologies and procedures subvert the benefits of enhanced security provided by Chip and PIN.

Chip and PIN. Almost every credit card issued in the U.S. is equipped with an EMV chip, or "Europay, Mastercard, and Visa" technology, and many also carry a mag stripe as well. The cards come in two flavors: Chip-and-Signature and Chip-and-PIN. Chip-and-PIN is the gold standard from a security standpoint and is used predominantly in Europe, where fraud rates are significantly lower than in the U.S. According to Barclays, the UK has fraudulent card transactions decline nearly 70 percent since adopting Chip & PIN cards.

However, Chip-and-Signature remains the preferred card type issued by FIs. Given the obvious security benefits, why is Chip & PIN not the standard in the U.S.? Some argue that the catch for American consumers is the inconvenience of having to remember and enter a PIN instead of just scribbling a signature. And for retailers, there can be additional costs associated with acquiring PIN devices, training staff, and educating users. For businesses like restaurants, which already operate on slim margins, the expense of installing dozens, hundreds, or even thousands of devices can be daunting.

Tokenization, simply put, is the process of exchanging a meaningful piece of data, like an account number, with a token or useless piece of information. When a consumer presents a tokenized payment card at the point of sale, the holder's primary account number is not exposed, so a fraudster has no incentive to go after the transaction. The information obtained, a random string of characters will be meaningless. The PIN is also not stored on the merchant's device, servers, or the servers controlled by the digital wallet provider. First introduced in 2001, digital tokenization is proven, secure, and trusted.

Tokenization is gaining popularity, at least by some card vendors. PayPal, Venmo, Zelle, Google Pay, and Apple Card, and Amazon Pay are examples of tokenized products.
We believe the U.S. must join with Europe, Canada, and most other developed nations to make Chip & PIN the standard retail payments device at the point of sale and support other products that use tokenization to enhance security. Fraud activity will diminish, and users will feel more secure.

4. EDUCATE CONSUMERS

The financial industry's primary goal is to move consumers to use more secure technology, such as mobile wallets and digital payments. Unfortunately, American consumers aren't on board. In an eye-opening Marqeta consumer survey , 80 percent of respondents stated, incorrectly, that a physical card is safer than a mobile wallet. At the same time, over half (54 percent) responded that fraud's risk made them less likely to try newer payment technology.

But 77 percent of respondents did say they would choose to shop at a merchant who did not store their information in favor of one that did. Indeed, 75 percent said they would be willing to manually enter their payment information repeatedly rather than have it stored by a merchant, indicating that the extra one-time step of loading a payment card in a digital wallet would not be a hurdle if security benefits were better known. In other words, they embrace tokenization, even if they're not sure of what it is or how it works.

These attitudes mark a massive failure to educate consumers on making more secure payments by both the financial industry itself and technology companies who sell these products. For example, consumers worried about protecting their personal data and guard against identity theft should know that when a payment card is tokenized and inserted into a digital wallet on a mobile device like a smartphone or smartwatch, it loses its value for fraudsters.

1. https://www.paymentsjournal.com/u-s-and-u-k-consumers-are-unprepared-for-the-new-world-of-digital-payments-how-tech-can-help/

Learn how to conquer digital payment by downloading our white paper Cyber Hygiene: How to Disinfect Digital Payments Against Fraud. https://www.capco.com/Intelligence/Capco-Intelligence/Cyber-Hygiene

You can also reach out to us directly at bryce.vandiver@capco.com or julien.bonnay@Capco.com to discuss how we can help your firm get on the path to building a resilient payments future.

WWW.CAPCO.COM

CAPCO

JN_2549