FIFTH THIRD BANK

Yikes! They really are out to get us. How to protect yourself from Commercial Cyber Crime and Identity Theft

Nick Ritter, SVP & Deputy Chief Information Security Officer

May 23, 2017

What's in the News?

Fraudsters Hit Businesses for Over $2.3 Billion in Email Scam

by Reuters APRIL 8, 2016, 4:34 AM EDT

Cases involved 17,642 businesses across 79 countries per the FBI.

Anti-Malware

DNC Breach More Severe Than First Believed

Jeremy Kirk • July 26, 2016

Fallout from the leaked Democratic National Committee emails continues, with a new finding that suggests cyberattackers compromised a staffer's personal email account. The FBI also has confirmed its ongoing investigation into the breach.

Anti-Malware

Omni Hotels & Resorts Hit by Hacker

Mathew J. Schwartz • July 11, 2016

Omni Hotels & Resorts is warning customers that for six months, hackers infiltrated its networks and used point-of-sale malware to steal payment card data. One security expert says more than 50 [illegible] stolen cards have been sold by a hacker called

Data Breach

$2.7 Million HIPAA Penalty for Two Sm[illegible] Breaches

Marianne Kolbasuk McGee • July 15, 2016

Oregon Health & Science University says it has been slapp[illegible] $2.7 million fine after HHS investigated two data breaches that affected a total of about 7,000 individuals. It's the eighth HIPAA-related settlement announced by HHS so fa[illegible]

Fraud

SWIFT Heists: The New Account Takeovers?

Tracy Kitten • July 25, 2016

An investigative report from Reuters paints a disturbing picture of the Federal Reserve Bank of New York using antiquated security practices to safeguard interbank SWIFT payments. Here's how security experts say interbank transaction security must be improved.

Data Breach

Wendy's Hackers Took a Bite Out of 1,000+ Restaurants

Jeremy Kirk • July 8, 2016

Nationwide fast food chain Wendy's has revised from 300 to 1,025 the number of restaurants that suffered payment card compromises. Investigators say the breach was more severe than they first believed, and involved two separate waves of point-of-sale malware attacks.

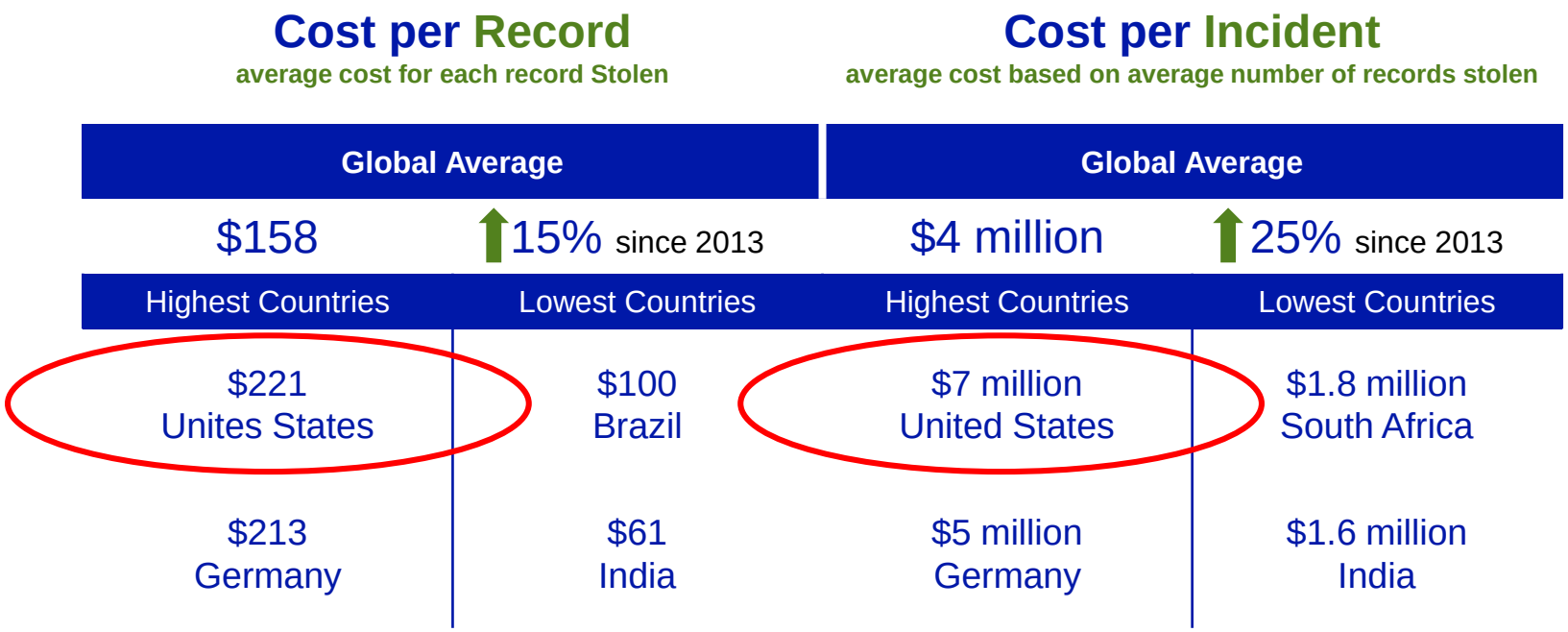
Cybersecurity

China Suspected in FDIC Breaches

Eric Chabrow • July 13, 2016

The Chinese government likely was responsible for the hacking of computers at the Federal Deposit Insurance Corp. in 2010, 2011 and 2013, according to a new congressional report. Also, a new audit from the FDIC inspector general criticizes the agency for continued lax information security practices.

The cost of a data breach continues to rise



Source: IBM/Ponemon Institute 2016 Study
All currencies converted to USD

Threats and the Human Element

Hacktivists

Directly attacks vulnerable systems of the targeted organization to cause disruption, embarrassment, and/or reputational harm

Criminals

Uses social engineering, phishing, and technical exploits to steal personal information, extort victims, and/or conduct fraudulent transactions

Espionage

Uses social engineering, phishing and technical exploits to steal sensitive or proprietary data, or cause disruption, to gain an economic advantage

Insider

Uses familiarity and knowledge of internal systems and processes to, intentionally or unintentionally, cause financial loss, disruption, or damage

Awareness and basic system hygiene will go a long way in reducing risk

Definitions:

- Social engineering: the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
- Phishing: the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Changing Threat Landscape

Established

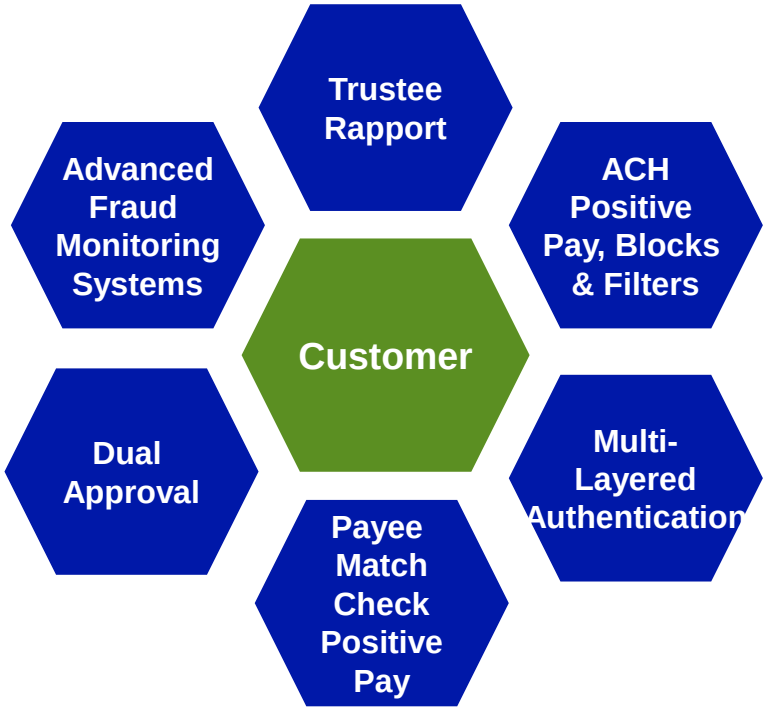
- Well-defined threat actor owning every stage in the “Kill Chain”
- Persistent attacks
- Well understood motives
- Parasitic model
- Externally focused
- Bounded IT environment

Emerging

- Threat marketplace
- Persistent AND multi-channel
- Nuanced or obscured motives
- Destructive model
- Internal and external
- Cloud, BYOD, SaaS, Mobile…

How Fifth Third Protects Both Our Customers and the Bank

At Fifth Third Bank, we take the security and confidentiality of your accounts and personal information very seriously. We are constantly enhancing our technologies, techniques, processes, and skills in support of our mission.



- Strong multi-factor authentication and fraud monitoring services
- Internal payment systems with built in segregation of duties processes

- Programs built upon the US National Institute of Standards and Technology (NIST) framework for Critical Infrastructure
- Constant Regulatory oversight to ensure adherence to framework and standards

Business Checklist

Just as the Fifth Third Bank team is committed to protecting both our clients and the enterprise, our business clients have similar obligations. Here are some highly effective actions businesses can take to protect their own network, company, and clients.

	What You Can Do		What You Can Do
❑	Install and regularly update security tools (anti-virus, anti-spyware, firewalls, etc.)	❑	Set up dual controls.
❑	If your company has internet sites, incorporate intrusion detection and vulnerability management tools.	❑	Use an up-to-date browser and apply patches regularly.
❑	Turn off and remove services that are not needed, like USB drives.	❑	Set rules about employee use of the internet.
❑	Make sure employee computer profiles have the least privileges possible.	❑	Never enter personal or customer-specific information into a public computer.
❑	Use a mail service that blocks or removes email file attachments commonly used to spread viruses.	❑	Make sure all employees use good security habits. Establish a security awareness program.
❑	Ensure only approved company applications are deployed and keep them patched.	❑	Consider adhering to an FBI recommendation for small businesses to dedicate one computer to handle online banking activity.
❑	Establish a procedure employees should use if they think their computer may be infected.	❑	Download the free Trusteer Rapport software available on our site to add another layer of security.
❑	Install pop-up blockers on your system.	❑	Review your account balance online on a daily basis to identify any fraudulent transactions.

Personal Checklist

In addition to the safeguards Fifth Third has put into place, being an educated consumer is your best defense. Below is a checklist of items that will help users know what to look for and what to do to protect both your personal informational and financial assets.

	Know What To Look For and What To Do		Know What To Look For and What To Do
❑	Beware of fraudulent emails. Never click on unverified links or attachments. Be wary if they include a sense of urgency.	❑	Keep all your software current. This includes security, browser, operating system and all other applications.
❑	Be on the lookout for spoofed or fake web sites.	❑	To be safe, always type the URL (e.g., www.53.com) in the address bar to access a web site.
❑	Do not use public computers and/or WiFi to access websites that require you to log in or to send sensitive information.	❑	Encrypt or mask sensitive information before sending it.
❑	Be aware of the potential for "shoulder surfers" when using your computer or mobile device in public.	❑	On mobile devices, only download information and apps from trusted sources, such as Google Play and Apple iTunes.
❑	Be cautious of unsolicited requests for information via email, text messages, or phone calls.	❑	Properly dispose of old computers and mobile devices. Use specialized software to erase all information prior to disposal.
❑	Monitor your online financial accounts frequently to identify unauthorized transactions. Leverage alerts.	❑	Report unauthorized transactions to your financial institution immediately.
❑	Check your credit report at least once a year. Leverage alerts.	❑	Use strong passwords, and do not use the same user ID and password on multiple sites.
❑	Look for "https" at the beginning of the URL before entering any sensitive or personal information.	❑	Password protect your mobile device and use its auto-lock feature.

THANK YOU