www.pwc.com

Cyber Fraud

March 2018

pwc

Agenda

Introduction

Defining Cyber Fraud

Fraud Landscape

Security Recommendations

Future Recommendations

Defining Cyber Fraud

Cyber Fraud in 2018

Cyber Fraud is Computer Fraud

- ❑ Cyber fraud combines cyber crime capabilities with traditional fraud motivations
  - ❑ The **U.S. Computer Fraud and Abuse Act** (**CFAA**) defines various fraud schemes in which a computer is accessed without authorization, or in excess of authorization.
  - ❑ Online fraud and subsequent financial crimes are elements of cybercrime
    - ❑ Leverage stolen Personally Identifiable Information (PII) and other data to commit further crimes

What are the immediate risks?

The motives of the attackers — either financially motivated attackers or nation-state actors — will determine how stolen PII could be used:

- ❑ **Financially motivated attackers:** If the attackers were financially motivated, they could use the stolen data to fraudulently open new accounts and gain access to existing ones. They may also seek to modify existing account information and gain access to additional PII. PII can be used for a wider variety of fraudulent purposes such as those listed below:
  - ○ Defeating existing identity verifications
  - ○ Creating and registering fraudulent accounts
  - ○ Changing passwords for online accounts
  - ○ Selling stolen information to other criminals
- ❑ **Nation-state actors:** If the attackers were nation-state cyber actors, the stolen data could be used for the following purposes:
  - ○ Building intelligence dossiers on individuals and organizations
  - ○ Conducting espionage

Cyber Fraud in 2018

Cyber Fraud is Profitable

- ❑ The quick adoption of new technologies, the ease of engaging in cybercrime, and the growing financial sophistication of professional cybercriminals led to a $16 billion profit from identify fraud alone in 2017.

Ransomware is the Fastest Growing Threat

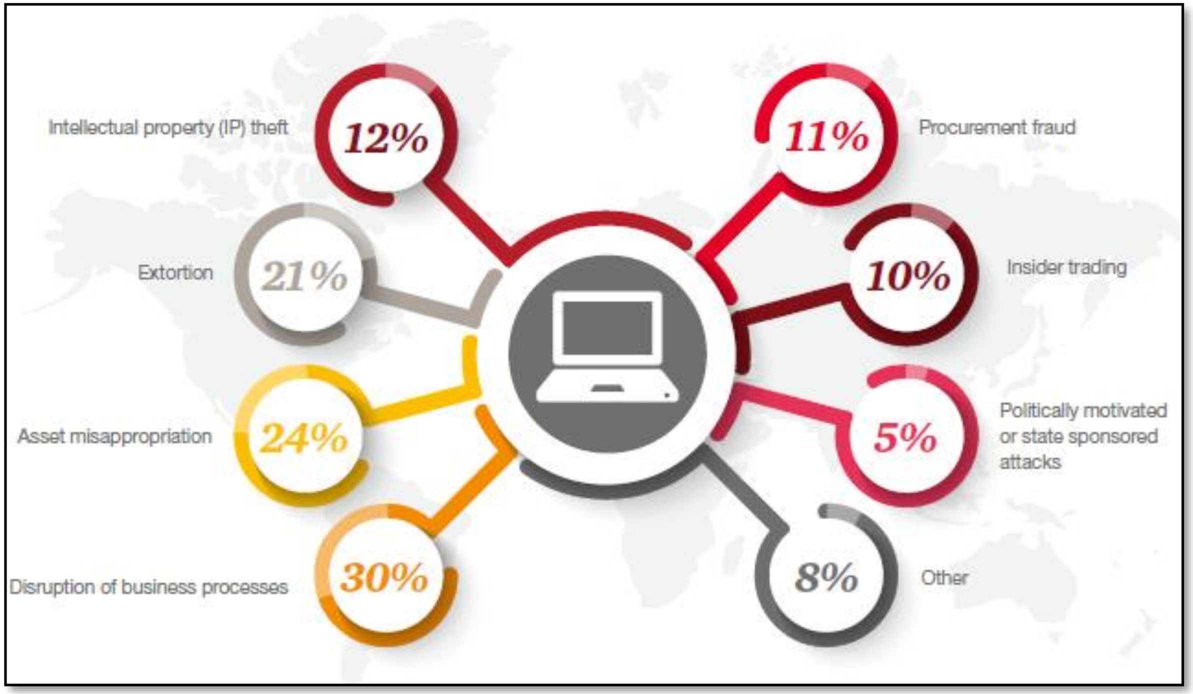
- ❑ Targets are universal—large enterprises to individual consumers
- ❑ In the first quarter of 2016 $209 million in ransom was paid in 2016 compared to $24 million in all of 2015.
- ❑ Ransomware tools are prevalent:
  - ❑ Over 6,000 online criminal marketplaces offer 45,000 different products and services

Source: The Economic Impact of Cybercrime— No Slowing Down

Fraud through Cyber-Attacks

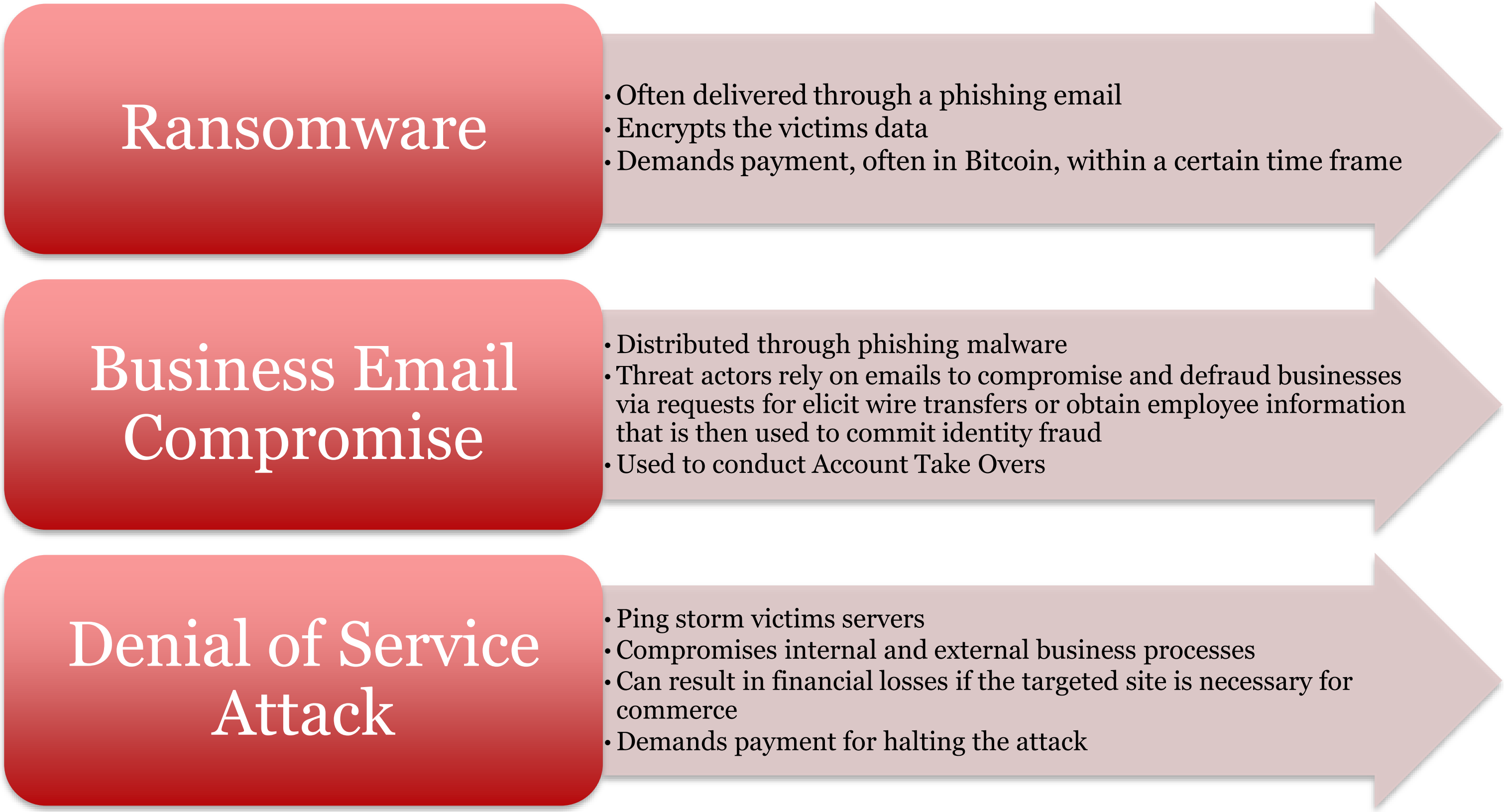
A recent PwC survey found the top three cyber frauds organizations faced were:

- ❑ **Disruption of business processes**
- ❑ **Asset misappropriation**
- ❑ **Extortion**



Cyber Fraud Techniques: Extortion

Financially motivated actors target customer and company data for extortion via Ransomware, Business Email Compromise, Denial of Service Attacks, and through Remote Access Data Exfiltration attacks



Ransomware

- Often delivered through a phishing email
- Encrypts the victims data
- Demands payment, often in Bitcoin, within a certain time frame

Business Email Compromise

- Distributed through phishing malware
- Threat actors rely on emails to compromise and defraud businesses via requests for elicit wire transfers or obtain employee information that is then used to commit identity fraud
- Used to conduct Account Take Overs

Denial of Service Attack

- Ping storm victims servers
- Compromises internal and external business processes
- Can result in financial losses if the targeted site is necessary for commerce
- Demands payment for halting the attack

Types of Account Takeover

- ❑ **Phishing Email:** Phishing emails entice employees or customers into taking actions designed to divulge sensitive information or install malware onto their computers.

- ❑ **“Man-in-the-middle” attack:** The attacker intercepts sensitive information, which allows them to alter sensitive information sent across the connection.

- ❑ **“Man-in-the-browser” attack:** The attacker exploits vulnerabilities in the browser by manipulating websites, allowing them to obtain and alter sensitive data fields in the website. These fields may include account login information, bank account numbers, and credit card numbers.

The fastest growing form of account takeover is ***business email compromise***, which uses an employee’s or customer’s hacked or spoofed email account to initiate fraudulent transactions.

Cyber Fraud Extortion in the News

Business Email Compromise

❑ In January 2018, PwC responded to a DocuSign-themed BEC compromise of a US business and found that dozens of users had navigated to a spoofed Office 365 login page and entered their credentials. One month prior, the same business fell victim to a fraudulent invoice scam delivered via spoofed messages from DocuSafe, a different digital invoicing vendor

❑ In the fourth quarter of 2017, the email security vendor Proofpoint reported that 89 percent of organizations were targeted with at least one BEC scam. Further, Proofpoint found that BEC incidents increased 17 percent from 2016 to 2017.

Trend Micro estimates cumulative losses from BEC scams will exceed $9 billion in 2018.

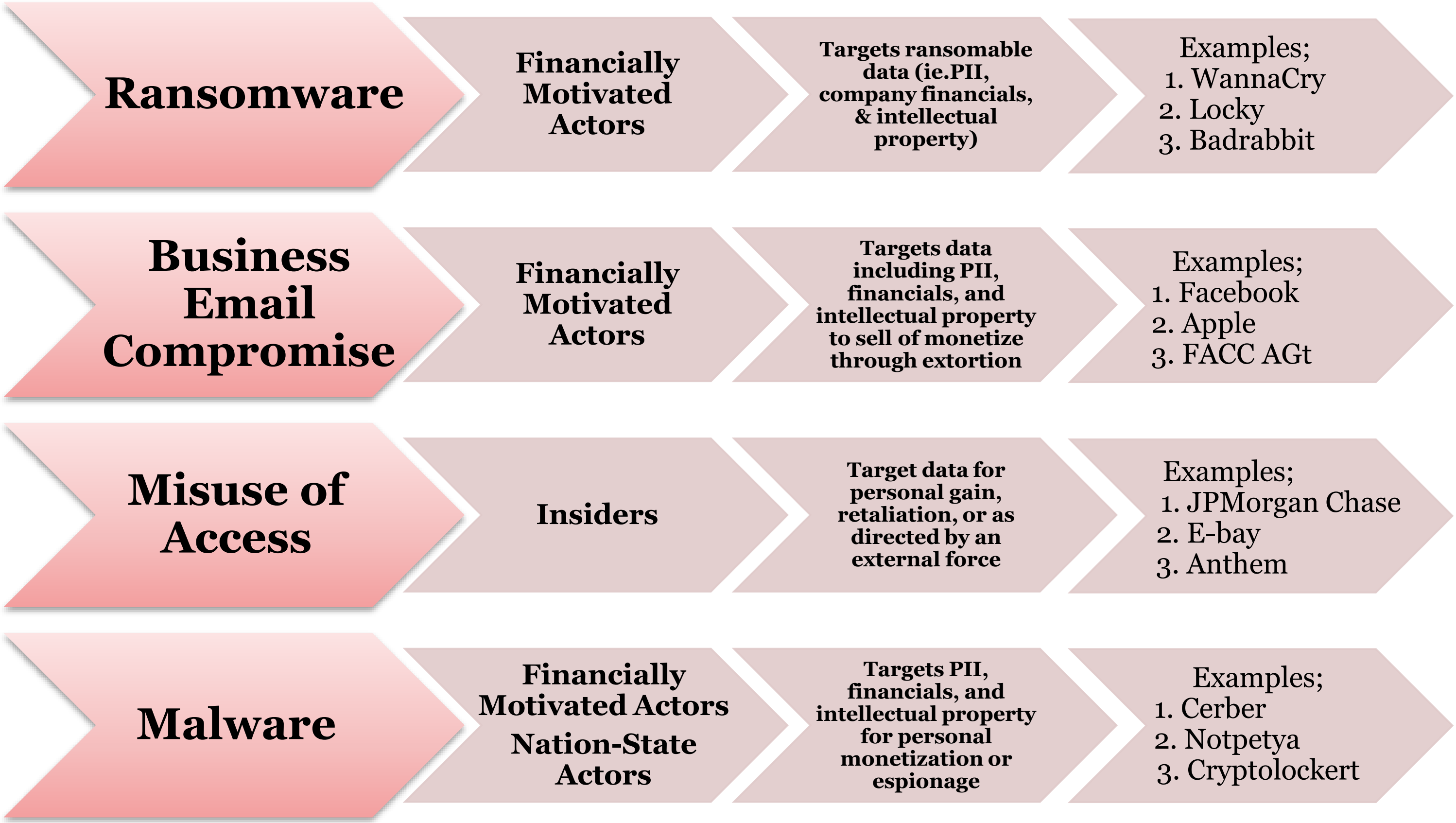
Ransomware

PwC in late 2017 investigated an AES Matrix ransomware attack on an east coast law firm. The threat actors gained access via brute force attacks against a server with an exposed Remote Desktop Protocol (RDP) port. and installed backdoors on two systems more than one month before the infection. The threat actor later utilized RDP access to install malware and run PowerShell scripts that enabled lateral movement to other systems on the network. The threat actor also used Mimikatz to dump user credentials. In total, the incident caused the victim over $750,000 in damages.

Data Theft

TheDarkOverlord (TDO) is a hacking group known to extort schools, healthcare providers, and businesses by stealing and threatening to release or sell data unless a ransom payment is made. According to the FBI, TDO has targeted at least 69 victims and attempted to sell over 100 million records. The group has also released 200,000 records because of victims refusing to pay.

Cyber Fraud: Data Exfiltration



Ransomware	**Financially Motivated Actors**	**Targets ransomable data (ie.PII, company financials, & intellectual property)**	Examples; 1. WannaCry 2. Locky 3. Badrabbit
Business Email Compromise	**Financially Motivated Actors**	**Targets data including PII, financials, and intellectual property to sell of monetize through extortion**	Examples; 1. Facebook 2. Apple 3. FACC AGt
Misuse of Access	**Insiders**	**Target data for personal gain, retaliation, or as directed by an external force**	Examples; 1. JPMorgan Chase 2. E-bay 3. Anthem
Malware	**Financially Motivated Actors** **Nation-State Actors**	**Targets PII, financials, and intellectual property for personal monetization or espionage**	Examples; 1. Cerber 2. Notpetya 3. Cryptolockert

Cyber Fraud Exfiltration in the News

Data Exfiltration: Securities Fraud

The criminal group FIN4, which began operating in mid-2013, is known to have compromised over 100 organizations to steal material nonpublic information used to enable insider trading. While it is unknown if this group remains active, we assess it is almost certain there are similar, unnamed groups seeking this type of information from public corporations.

A 2017 industry survey found that 92 percent of IT security professionals have caught employees attempting to access information outside the information needed for the employee's day-to-day work

Insider Threat: Personal Gain

In January 2018, a terminated database manager with the Department of Veterans Affairs (VA) attempted to sell the personal information of veterans and VA employees for personal gain. The employee maintained VA property in his possession following his termination and was able to remotely access the VA systems.

Nation-State Actors: Espionage

Chinese espionage actors have historically targeted food sciences and global supply chain data. In 2010, Chinese hackers conducted intrusions into multiple law firms, financial institutions, and public relations firms to collect information relating to a company's potential acquisition of Potash Corp., the world's largest producer of the water-soluble form of potassium used in fertilizers.

Fraud Landscape: 2018

Fraud Landscape - 2018

Below are our ***five*** considerations in the fraud landscape this year, including emerging threats, industry developments, and next steps:

- ❑ Account opening fraud and account takeover risk will continue to rise, driven chiefly by digital data theft.
- ❑ Data privacy, security, and fraud risk management standards in the US will be refined and possibly adopted nationally.
- ❑ The adoption of new authentication techniques, including biometrics, will continue to grow in an effort to counter the trend.
- ❑ Financial institutions and others will use RPA to enhance fraud management effectiveness.
- ❑ The industry will increasingly use artificial intelligence, but fraudsters will too.

Key Challenges for Fraud Management

The most significant challenge we see in achieving a sound fraud management operating model stems from:

- ❑ Functional silos for fraud prevention and detection of malicious activity
- ❑ Clearly defining roles and responsibilities for fraud prevention and detection functions
- ❑ Ensuring that all three lines of defense are working together effectively and not duplicating roles
- ❑ Navigating the vast and constantly evolving universe of fraud risks
- ❑ Not enough resources to fully assess the fraud risks and tend to focus their efforts on highly publicized external fraud risks such as business email compromise and account takeover, and often miss key threats facing their organization

Security Recommendations

Mitigating Cyber Fraud

What Should Firms be Doing to Combat Account Takeovers?

There are a number of steps firms can take to combat account takeover:

1. ***Payment Controls:*** Some payment control techniques include requiring multiple approvals for large transactions, reviewing changes in payment instructions and counterparty information, and carefully scrutinizing international wire transfers.

2. ***Enhanced fraud detection and analytics:*** An automated real-time monitoring system correlating data points generated by various payment, customer, transaction, and compliance systems can use data analytics and predictive algorithms that identify patterns and anomalies that indicate fraud. Additionally, firms can use these systems to detect the root cause of successful attacks and develop new scenarios to identify emerging account takeover trends.

3. ***Threat intelligence:*** Threat intelligence services use shared knowledge from various internal and external resources to prevent and detect attack. This intelligence is both tactical and strategic and stems from collecting data points regarding known attackers, malware, and vulnerabilities from the entire industry. This service can be combined with data analytics and automated fraud detection systems to identify and prioritize threats.

Keeping your organization safe

Institutions should have a robust understanding of the threat actor's cyber kill chain

- ❑ Implement and establish three lines of defense framework and operating model
- ❑ Identify resources for identification and prevention at each stage
- ❑ Plan accordingly to mitigate any attacks that evade early detection
- ❑ Ensure the incident response team can restore business operations to pre-incident levels

What should organizations be doing post breach?

- ❑ Identify at-risk customers
- ❑ Communicate with clients
- ❑ Enhance cybersecurity and fraud controls
  - ❑ Cybersecurity controls
  - ❑ Anti-fraud controls
- ❑ Integrate cybersecurity and fraud programs

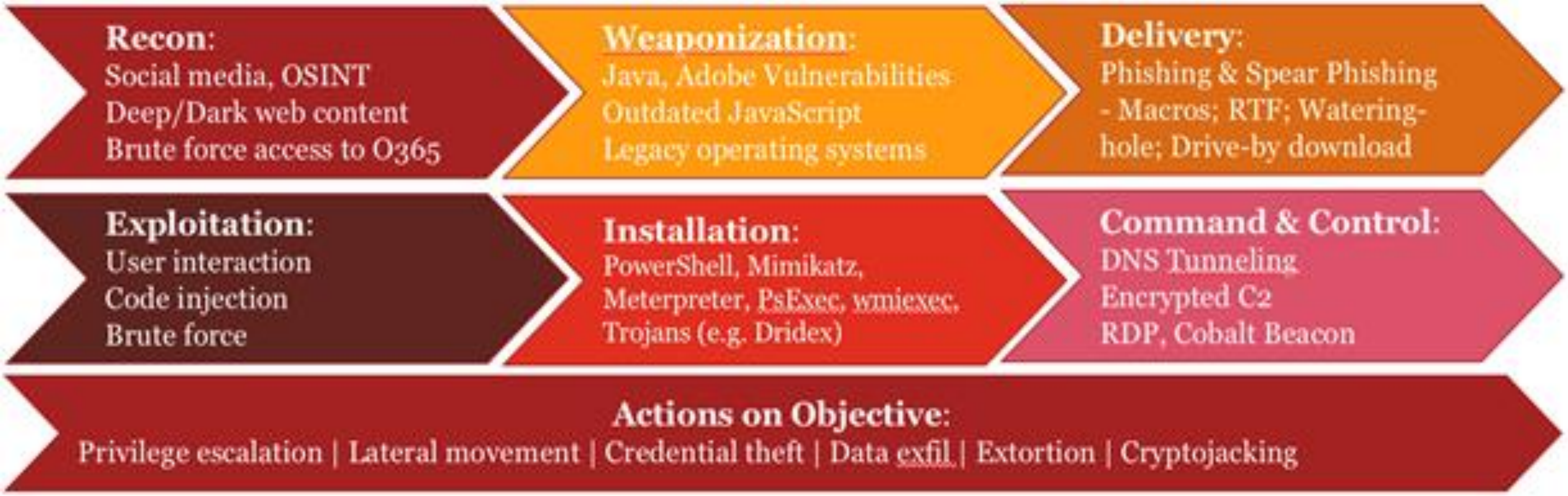
Compliance departments should closely follow federal and state regulations that may require that they inform customers or regulators within a prescribed time period.

Thank you

At PwC, our purpose is to build trust in society and solve important problems. PwC is a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/us.

Appendix

Cyber Kill Chain



Recon:
Social media, OSINT
Deep/Dark web content
Brute force access to O365

Weaponization:
Java, Adobe Vulnerabilities
Outdated JavaScript
Legacy operating systems

Delivery:
Phishing & Spear Phishing - Macros; RTF; Watering-hole; Drive-by download

Exploitation:
User interaction
Code injection
Brute force

Installation:
PowerShell, Mimikatz, Meterpreter, PsExec, wmiexec, Trojans (e.g. Dridex)

Command & Control:
DNS Tunneling
Encrypted C2
RDP, Cobalt Beacon

Actions on Objective:
Privilege escalation | Lateral movement | Credential theft | Data exfil | Extortion | Cryptojacking

Criminal Threat Actors' Cyber Kill Chain