



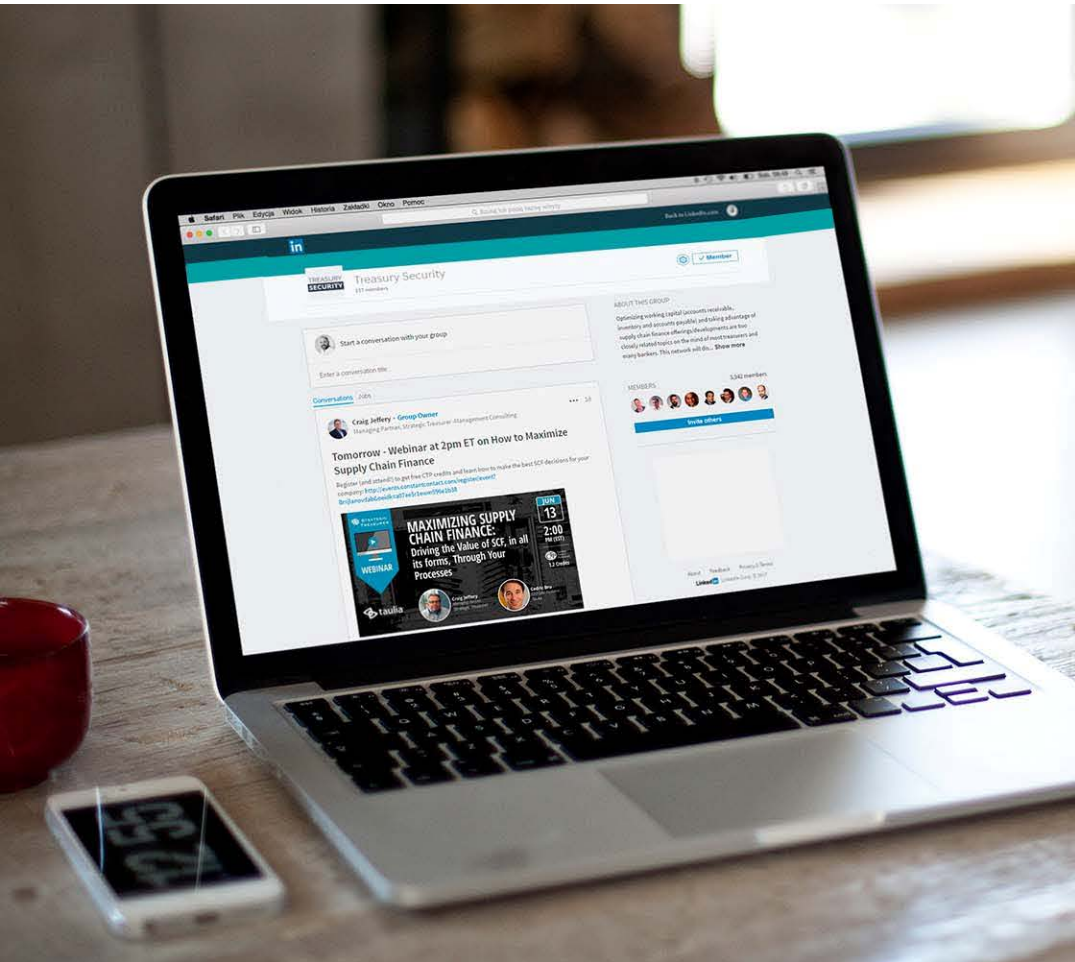
# The Evolution of Fraud

The Rise of Ransomware and Imposter Fraud

June 2017

Presented By:







## About the Presenter



*Today's Co-Presenter:*

**Craig Jeffery, CCM, FLMI**  
*Founder & Managing Partner*  
**Strategic Treasurer**

**Craig Jeffery** formed Strategic Treasurer LLC in 2004 to provide corporate, educational, and government entities direct access to comprehensive and current assistance with their treasury and financial process needs. His 20+ years of financial and treasury experience as a practitioner and as a consultant have uniquely qualified him to help organizations craft realistic goals and achieve significant benefits quickly









**Strategic Treasurer** was founded in 2004 by Craig Jeffery, a financial expert and trusted advisor to executive treasury teams since the early 1980's. Partners and associates of Strategic Treasurer span the US, the UK, and continental Europe.

This team of experienced treasury specialists are widely recognized and respected leaders in treasury and risk management technology consulting. Known for their expertise in treasury technology, risk management, and working capital as well as other cash management and banking issues, they efficiently identify issues, creatively explore ideas and options, and provide effective solutions and implementations for their valued clients.





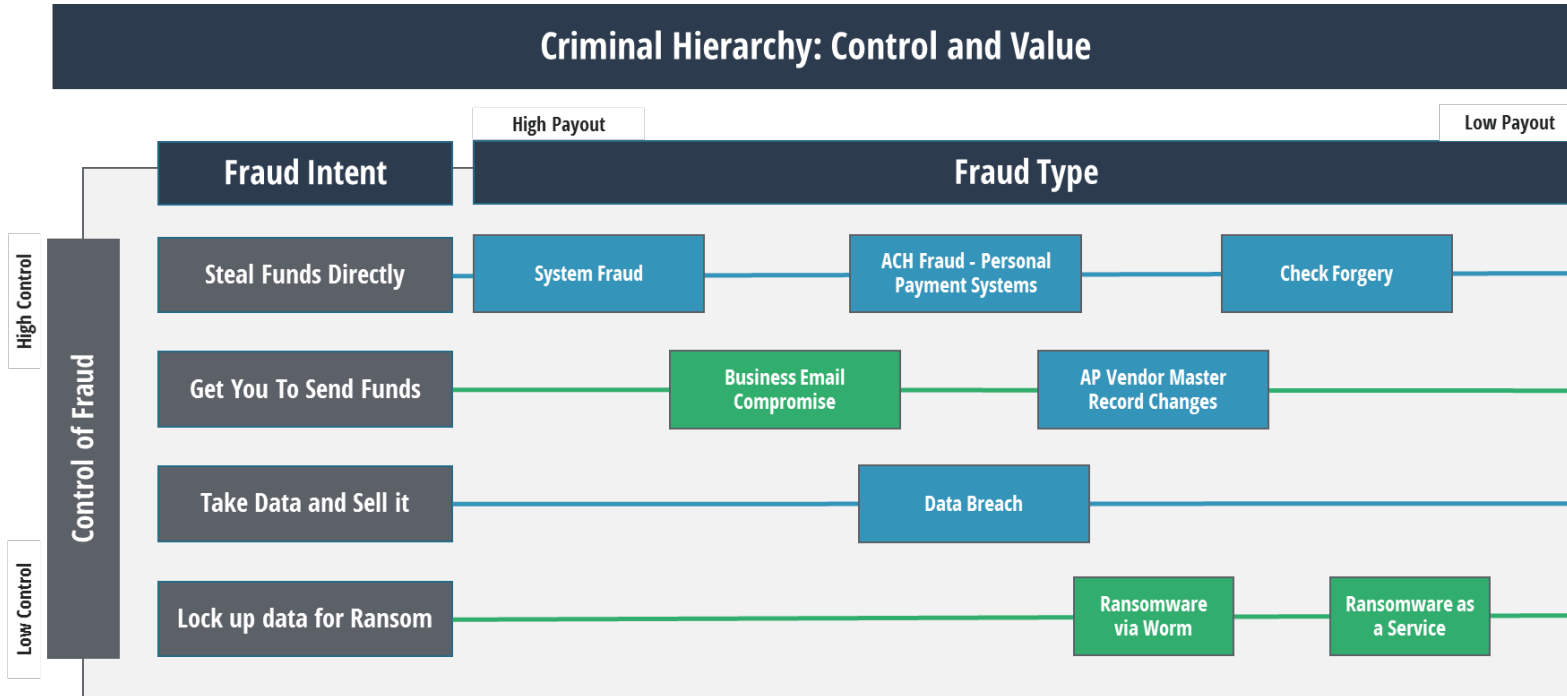
## Topics of Discussion

-  **Intro to Corporate Fraud: The Criminals' Playbook**
-  **Fraud in Focus: Imposter/BEC Fraud**
-  **Fraud in Focus: Ransomware**
-  **Industry Examples: Fraud Cases**
-  **Fraud Prevention Playbook: An Updated Fraud Prevention Approach**
-  **Key Takeaways, Q&A**





# Corporate Fraud: The Fraud Landscape

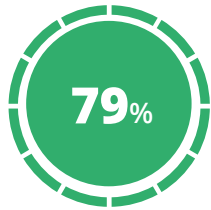




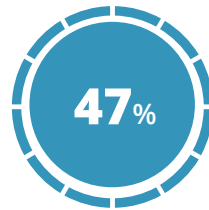
## Corporate Fraud: Frequency of Attacks



Of firms have experienced either payment fraud, cyber fraud, BEC/imposter fraud, or ransomware attacks within the past two years.



Have experienced BEC/imposter fraud attempts within the past two years.



have experienced cyber fraud attacks within the past 12 months



have experienced payment fraud attempts within the past 12 months.



have experienced ransomware attacks within the past two years.



## Corporate Fraud: Criminal Success Ratios

The number of **successful fraud attempts**, specifically imposter fraud and ransomware, **are increasing** as criminals identify corporate exposure points.



### BEC/Imposter Fraud

- 79% of firms were targeted through BEC/Imposter fraud schemes in 2015-16.
- 1 in 7 firms targeted through BEC/imposter fraud suffered a loss.
- The average payout for a successful BEC attempt in the US is \$130K.






### Ransomware

- 8% of firms experienced ransomware attempts in 2016.
- In 2017, Ransomware has become one of the most feared types of fraud due to several high-profile cases.
- Only 39% of those hit with ransomware attacks have sufficient backups to restore their data.
- Nearly 1 in 9 firms targeted through ransomware lose significant data.



## Fraud in Focus: BEC/Imposter Fraud

**BEC/Imposter Fraud** involves a criminal **imitating or impersonating** a corporate employee or business partner in an attempt to **convince an employee** to initiate a **funds transfer to a fraudulent account**.

-  Often initiated by criminals via emails or phone calls to company staff.
-  Criminals may pretend to be an employee, or an employee from a business partner, such as a vendor or bank.
-  Criminals will use fake credentials or email addresses to disguise themselves in an attempt to convince an employee to initiate a funds transfer to their fraudulent account.





## Fraud in Focus: BEC/Imposter Fraud Steps

 **Assume Control.**

 **Mimicry.**

 **Timing.**

 **Act.**

 **Urgency.**

 **Escape.**





## Fraud in Focus: BEC/Imposter Fraud Case Study

- **Context**
- **What happened?**
- **Where did the exposure arise?**
- **What was the end result?**
- **Practical Takeaways**





## Fraud in Focus: Ransomware

**Ransomware** involves a criminal or group of hackers **infiltrating the systems** of an organization and **stealing or capturing data**. Hackers will then **hold data for ransom** and coerce employees into **making a payment** to get their information back.



A drastic increase in ransomware activity has occurred thus far in 2017.



Ransomware is a unique type of fraud in that it does not specifically target money.



If organizations do not back up their files, they risk losing significant data.



## Fraud in Focus: Ransomware Steps



**Infiltrate Security.**



**Alter Access Codes or Encrypt Data.**



**Restrict System Entry.**



**Request Payment in Exchange for Data .**



**Receive Payment (Bitcoin/Cryptocurrency).**



**Escape or Simply Remain Anonymous.**



## Fraud in Focus: WannaCry Ransomware Attacks

- **WannaCry is an ongoing ransomware epidemic that first appeared earlier this year.**
- **WannaCry is a spinoff of EternalBlue, a tool originally built by the NSA.**
- **WannaCry works by exploiting weaknesses in a user's Windows operating system in order to obtain and then encrypt files.**
- **Once files have been encrypted, the hackers demand a ransom in order for the user to regain access to them.**
- **As recently as this week, Honda was forced to shut down a plant in Tokyo due to a network breach.**
- **Similar attacks have hit companies including Netflix and Disney in the past several months.**



## Fraud Prevention: The Use of a New Playbook

- ✓ The use of new fraud techniques means firms must **update their fraud prevention strategies and security tools.**
- ✓ **Provide regular training & testing of employees on how to identify and react to specific types of fraud (i.e. a suspicious email).**
- ✓ Always ensure that company data is **backed up on a separate system or hard drive. Only 39% of firms affected by ransomware had adequate backups.**
- ✓ **Undergo regular treasury security assessments (internal and external) to ensure operations are secure and updated. New fraud methods arise rapidly.**
- ✓ **Have a pre-planned response strategy for effectively dealing with fraud attacks; the quicker the response, the fewer losses sustained.**



# The Four Pillars of Treasury Security



## FOUR PILLARS of TREASURY SECURITY

### 1. ASSESS & ARCHITECT

- Greater Awareness

### 2. PREPARE & PREVENT

- Stronger Defense Posture

### 3. MANAGE & MAINTAIN

- Ongoing Training
- Testing

### 4. RESPOND & RECOVER

- Reporting
- Response (Fast, Appropriate, Lockdown)
- Rework (Restore to New Operating Model)



## Action Items



1. **Perform:** Fraud/Security Assessments, Review Layers



2. **Compare:** Benchmark Key Areas



3. **Create:** Treasury Security Framework



4. **Calibrate:** the proper level of response



5. **Communicate:** Treasury Security Framework



6. **Train:** Find opportunities to have regular training.







## Q&A





Craig Jeffery, CCM, FLMI  
*Founder & Managing Partner*  
*Strategic Treasurer*

Email: [craig@strategictreasurer.com](mailto:craig@strategictreasurer.com)

Direct: +1 678.466-2222

### **Strategic Treasurer**

is a consulting firm advising on treasury, financial risk and risk technology issues. Their seasoned treasury consultants efficiently work alongside financial executives in treasury, finance, and other related areas within corporate, government, education, and not-for-profit entities.