Cybersecurity Incident Response

January 2019

John Lawrence and Jay Wiley

M&T Bank

Overview and Refresher

What is Cybersecurity?

Cybersecurity programs maintain three core principles in order to protect data and systems

- **Confidentiality** — Data is only accessible to those authorized, information kept private and secure
- **Integrity** — Data is accurate and transactions can only be performed by those with authorization
- **Availability** — Data is accessible when it is needed

Hacker Motivation – Who and Why?

Reduced R&D
Political embarrassment, brinksmanship

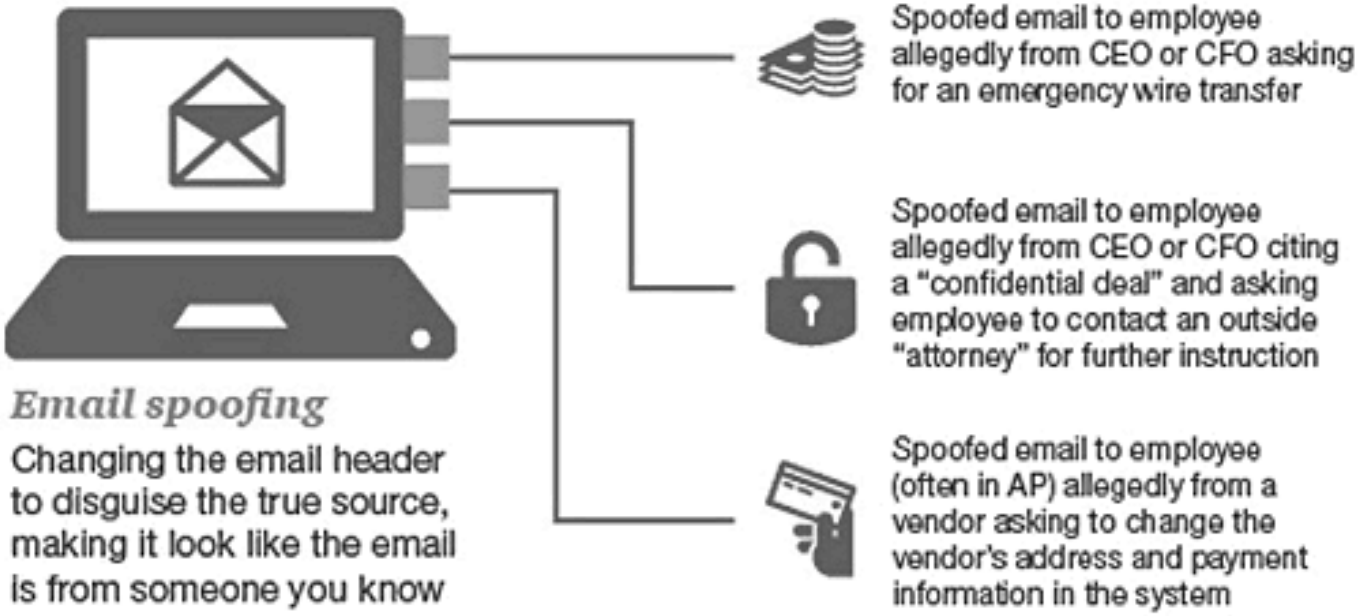
Retaliation
Advantage for a new employer
Financial gain

Financial gain
Power

Notoriety, either personally or for a cause
Punishment for perceived wrongdoing

Executive Impersonation Fraud: What is it?

Cyber criminals impersonating senior level officials via email in an attempt to trick a member of that financial institution into sending money by wire or ACH



Executive Impersonation Fraud: Real-Life Scenario

Hundreds of millions of dollars are stolen each year by wire fraud, with executive impersonation attempts continuing to rise. What better way to drive home the importance of organizations consistently demonstrating the right behaviors than to view a real-life example of an executive impersonation wire fraud that was successful.

The Scene

The Controller of XYZ Company is forwarded an email exchange between her CEO and CFO, in which the CFO instructs her to originate a wire transfer out of their business account. The Controller complies with the request and receives a wire call back from M&T Bank to confirm the instructions.

Cast

Tim Smith……XYZ Company CEO

David Jones……XYZ Company's CFO

Gina Green……XYZ Company's Controller

Note: All names and client information have been changed to protect the parties.

-------- Original Message --------

Subject: Wire Payment
Date: 2015-05-29 10:44
From: Tim Smith <Tim. Smith@XYZCompany.com>
To: David Jones <David.Jones@ XYZCompany.com>

David,

Per our conversation, attached is the wiring instructions. As you already know, the support for this will come in handy later. Let me know once this is processed.

Tim

From: David Jones [mailto:david.Jones@XYZCompany.com]
Sent: Friday, May 29, 2015 1:55 PM
To: Green, Gina (Anywhere)
Subject: Fwd: Wire Payment

Gina,

Are you able to process an international wire before the cutoff time?

David

On 2015-05-29 19:22, Green, Gina wrote:

For how much?

Gina Green
Gina.Green@XYZCompany.com
555-828-8366 (Office)
888-555-1059 (Fax)
199 Blank Street, Suite 800
Anywhere, NY 12345
www.XYZCompany.com

From: David Jones [mailto:david.Jones@XYZCompany.com]
Sent: Friday, May 29, 2015 3:27 PM
To: Green, Gina
Subject: RE: Wire Payment

$314,701.65.

On 2015-05-29 19:28, Green, Gina (Anywhere) wrote:

Ok. Is this supposed to be out of our M&T lockbox account? Do you have a free moment to call my cell 555.913.8568?

Gina Green
Gina.Green@XYZCompany.com
555-828-8366 (Office)
888-555-1059 (Fax)
199 Blank Street, Suite 800
Anywhere, NY 12345
www.XYZCompany.com

From: David Jones [mailto:david.Jones@XYZCompany.com]
Sent: Friday, May 29, 2015 3:39 PM
To: Green, Gina (Anywhere)
Subject: RE: Wire Payment

Can it wait? What's the issue?

From: Green, Gina
Sent: Friday, May 29, 2015 3:51 PM
To: 'David Jones'
Subject: RE: Wire Payment

You answered my question. I just need to understand this a bit better because in order to be paid out of the lockbox it needs to be paid into that account in the first place. I have approved the wire, so it is submitted.

Gina Green
XYZCompany
Gina.Green@XYZCompany.com
555-828-8366 (Office)
888-555-1059 (Fax)
199 Blank Street, Suite 800
Anywhere, NY 12345
www.XYZCompany.com

From: Green, Gina [mailto:Gina.Green@XYZCompany.com]
Sent: Monday, June 01, 2015 3:10 PM
To: M&T Bank Relationship Manager; TM Consultant; Relationship Liaison
Subject: FW: Wire Payment
Importance: High

The wire that was sent on Friday was completely bogus. I need it pulled back immediately. Please call me ASAP.

Thank you,
Gina

Gina Green
XYZCompany
Gina.Green@XYZCompany.com
555-828-8366 (Office)
888-555-1059 (Fax)
199 Blank Street, Suite 800
Anywhere, NY 12345
www.XYZCompany.com

Click here to listen to recording of the M&T wire room call back conversation

M&T Bank

Executive Impersonation Fraud: How Does it Happen?

- An increase in **malware** is being used in connection with Impersonation scams
- Email accounts are **hacked** or email addresses are made to appear very similar
- Instructions are often purported to be **urgent** or confidential
- Spoofed emails very closely **mimic** a legitimate email account or recent request
- Email recipients are usually **authorized** to initiate payments, such as web based banking application user or an authorized signor on an account
- Many times, the transactions are sent to **international** banks in China or Hong Kong
- Fraudsters may pose as lawyers who claim to be handling **confidential or time-sensitive** information.

Third-Party Risk

Spectrum of Control Environments:

- **Weaker:** may need to share information with a company with weaker controls if it provides a unique and necessary service
  - Smaller vendors are often targeted by cyber criminals for this reason
- **Stronger:** Large and highly complex vendors may maintain a stronger control environment

Numerous successful cyber attacks against major companies have been associated with third parties

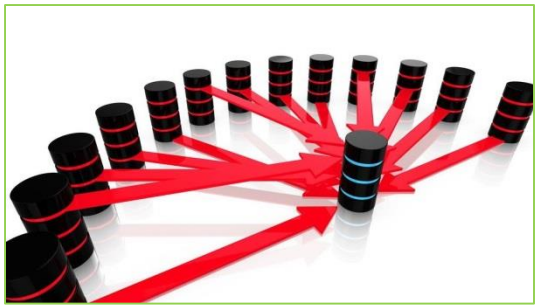
Challenges:

- **Limited Oversight:** It is difficult to assess the strength of a third party control environment without a direct sightline into a company's Information Security Program
- **Limited Control:** Shared services and contractual obligations with long-term relationships may limit the ability to require new controls around information security
- **Regulatory:** Numerous third party incidents have made this an area of significant interest to regulators

Defenses:

- A robust **Cybersecurity Due Diligence** process helps ensure vendor relationships do not pose unnecessary or excessive risk to the corporation.
  - Incorporated into Procurement's Third Party Risk Management Process
  - Cybersecurity employees perform tiered levels of due diligence aligned to the risk associated with each business relationship
  - Cybersecurity is the highest weighted component of overall third party risk

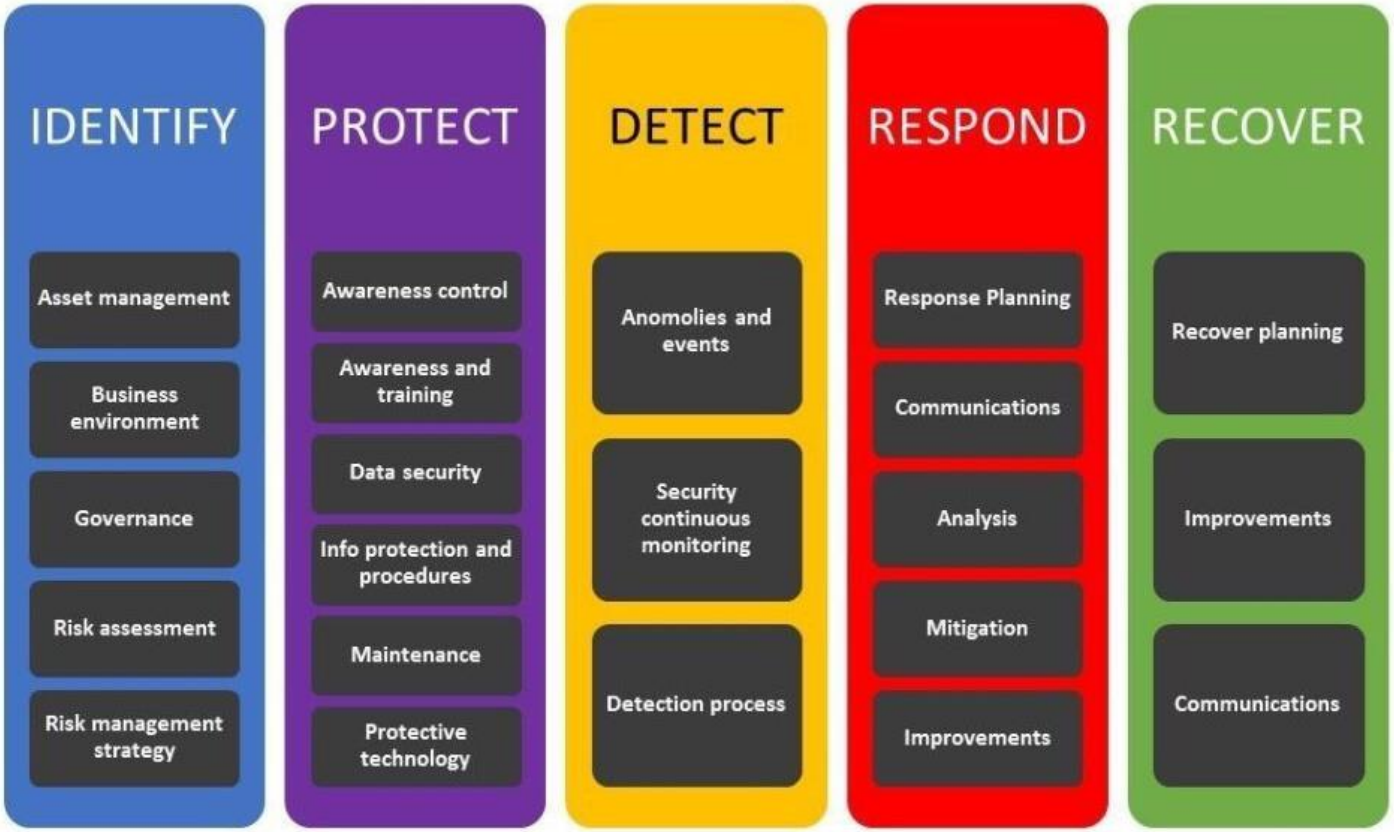
Other Trends in Fraud



M&T Bank

Incident Response

National Institute of Standards (NIST) Framework



M&T Bank

Understanding what's important®

Computer Incident Response Team Process

Version 4.1

August 24th, 2018

CIRT Process Management:
CSOC@mtb.com / 844-440-2762 / 001-302-934-2104 (international)

Importance of CIRT Team Participation

- Who needs to be on?
- What will they bring to the table?
- Where does the team meet?
- When does the team meet?
- Why do they need to be on?
- How will they be engaged to join?

Legal	Insurance
Risk	HR
Audit	Privacy
Communications	Incident Management
Technology	Affected Business Units

Roll Call

1 Establish the call

Roll Call

CIRT Situational Awareness Team for Priority 2:

- Director of Cybersecurity Operations (Incident Manager)
- Cybersecurity Operations Center (CSOC)
- Cybersecurity Network Defense
- Cybersecurity Advanced Threat Hunting Team
- Threat Intelligence Officer
- Infrastructure Command Center (ICC)
- Technology Services & Operations
- Technology Engineering
- Incident Management
- Help Desk
- Financial Crimes
- Disaster Recovery/Business Continuity
- IT Audit
- Telecommunications
- Privacy Office/Compliance
- Technical Risk Management
- Operational Risk Management
- Corporate Insurance
- Third Party Risk Management
- Legal Counsel

CIRT Situational Awareness Team for Priority 1

For Priority 1 Team, Please Also Include the Above Members Listed in Priority 2:

- Physical Security and Investigations
- Banking: Commercial, Business, Digital, and Retail
- Human Resources
- Corporate Communications
- Wilmington Trust (wt.com)
- Item Processing
- Payment Services
- SWIFT
- Customer Contact Center

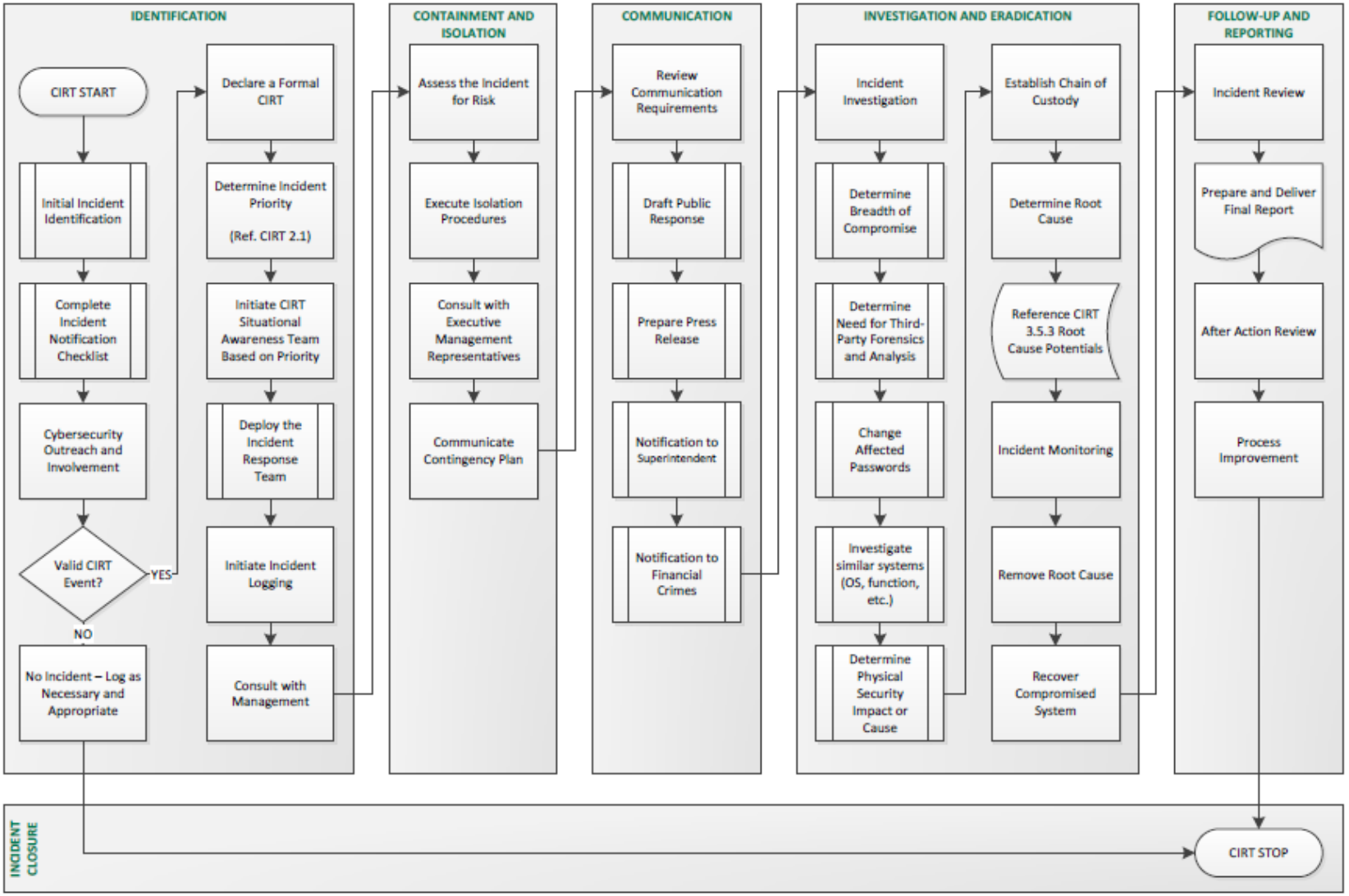
IR Call Script

- Establish the call
  - Pre-defined rolls based on priority
- Situational Update
- Risk Assessment
  - Customer, Reputational, Business, Technical, Regulatory, etc.
- Investigation Steps
  - Common and event-specific
- Recovery
  - Change control
- Wrap Up / Lessons Learned

Categorization Table

Factor	Description	Low	Moderate	Severe	Significant
Financial	*Direct and indirect financial impacts including direct cash outflows, lost opportunity for new business/revenue, fines and unrealized benefits.*	*Thousands of Dollars*	*Up to One Million Dollars*	*Up to Ten Million Dollars*	*Over Ten Million Dollars*
Reputational	*Reputational damage with a direct or indirect impact to shareholder value of the brand.*	*No / minimal reputational impact*	*Low Media Buzz*	*Media Reports*	*Media Headlines*
Regulatory	*Regulatory censure, loss or restriction of the ability to conduct business in a state, territory or country. Actions that cause regulatory special audit.*	*No / minimal regulatory impact*	*Regulatory concerns*	*Regulatory Notification Required*	*Regulatory Notification Required / Scrutiny May Be Received*
Customer	*Negative customer impact including inconvenience and/or service disruption.*	*No / minimal customer impact*	*Low Customer impact*	*Multiple Customers impacted*	*Multiple Customers impacted*
Operational	*Negative employee impact, inconvenience and/or service disruption.*	*No / minimal impact on BAU support functions and/or operations.*	*Low impact on BAU*	*Impact on Several BAU Tasks*	*Widespread / Bank wide impact on BAU tasks*
Severity	**Description**	**Severity / CIRT 4**	**Severity / CIRT 3**	**Severity / CIRT 2**	**Severity /CIRT 1**
Business Impact	*Potential for current status and impact to degrade to the point of service disruption or full outage. This includes consideration of financial, reputational, regulatory, customer and operational impacts.*	*Limited disruption that do not carry risk of a service outage. Minimal to no risk to SLAs or other time sensitive processes.*	*Disruption of secondary or supporting functions that do not carry risk of a service outage.*	*Moderate to high impact on service availability.*	*High impact to multiple LOBs and/or products. Critical SLAs or other time-sensitive processes will not meet prescribed deadlines.*
Technological/ Cybersecurity Assessment	*Potential for current status and impact to degrade to the point of service disruption or full outage. This includes consideration of financial, reputational, regulatory, customer and operational impacts.*	• *Loss of Employee IT Asset* • *Low-risk vulnerability / patching* • *Threat of Compromise*	• *Denial of Service attack* • *Email-Abuse campaigns* • *Moderate-risk vulnerability / patching* • *Theft of bank data* • *Credential stuffing attack*	• *Insider Threats* • *Loss of Bank-owned hardware* • *High-risk vulnerability / patching* • *Network Intrusion* • *Malware*	• *Widespread System Compromise* • *Customer Data Compromise* • *Ransomware* • *Website Defacement*

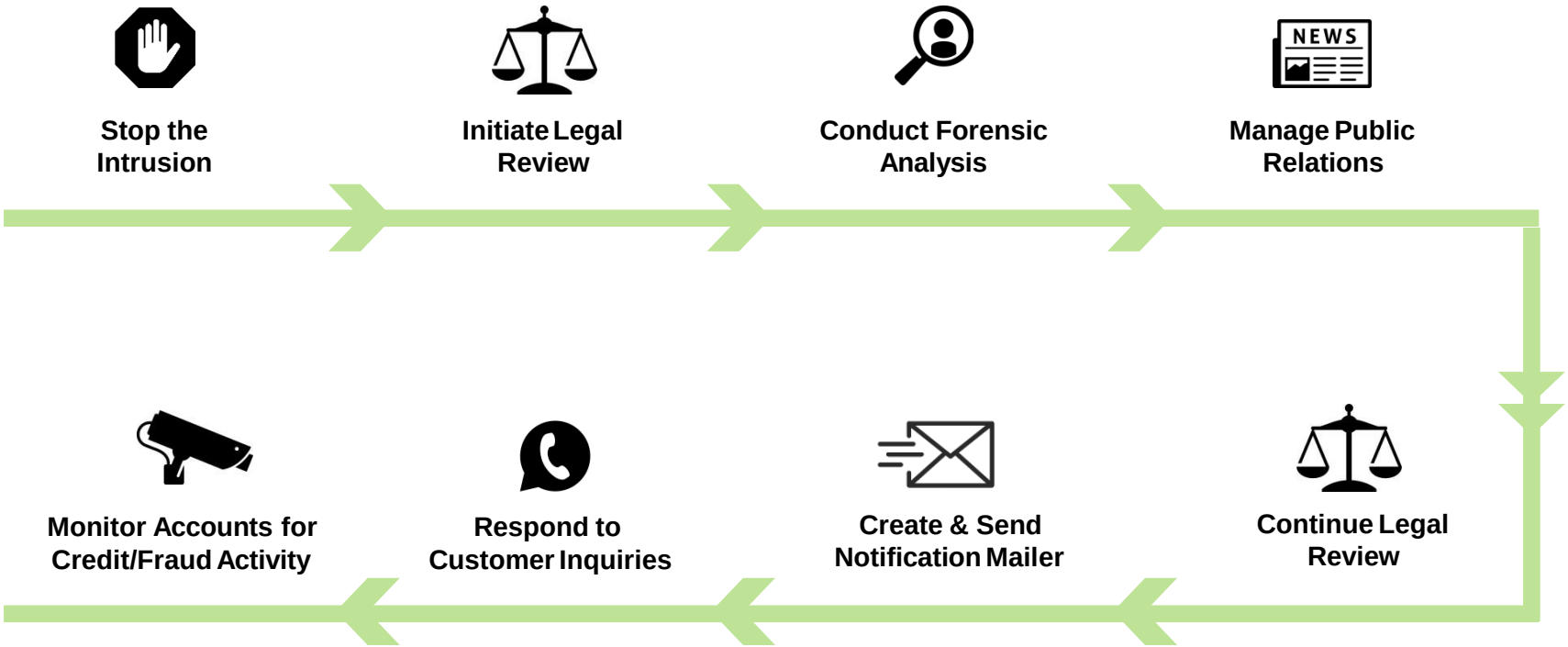
Process Flowchart



M&T Bank

Risk Management Activities

Response – Data Breach Response Cycle



Things to Consider

- **Automation**
- Federal and State Reporting requirements
- ***Preparation***
- **Legal Privilege**
- *Insurer requirements*
- DR/BC Coordination makes this easier
- If applicable, GDPR

Questions?

Thank You!