BIG UNIVERSITY 2018

BIG UNIVERSITY 2018

Owner / Principal Track

SESSION 1

Disaster Recovery - A Case for Business Continuity Management

JD Mulliken (Paytime)

Agenda

- Why, what happened?
- Terminology
- Strategies and Processes
- Establishing a Framework
  - Assessment and Objective Setting
  - Critical Process Identification
  - Business Impact Analysis
  - Continuity Response Approaches
  - Plan Implementation and Testing
  - Monitoring, Validating and Improving
- A guide to creating a ‘Run Book’
- Additional Resources and References

A Travelers study found that 48% of small businesses are operating without any type of business continuity plan, yet 95 percent indicated they felt they were prepared.

-Travelers Insurance (2012)

Business Continuity Institute - Horizon Scan Report 2018

Top 10 threats

2 Data breach

3 Unplanned IT and telecom outages

4 Interruption to utility supply

5 Adverse weather

6 Act of terrorism

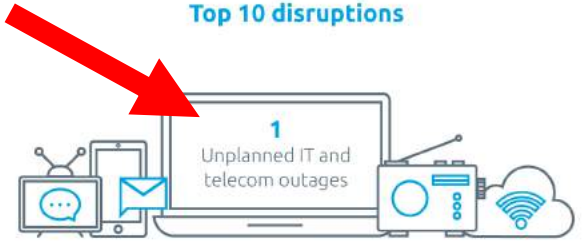
7 Security incident

8 Fire

9 Supply chain disruption

10 Transport network disruption

Top 10 disruptions



2 Adverse weather

3 Interruption to utility supply

4 Cyber attack

5 Availability of talents/key skills

6 Security incident

7 Transport network disruption

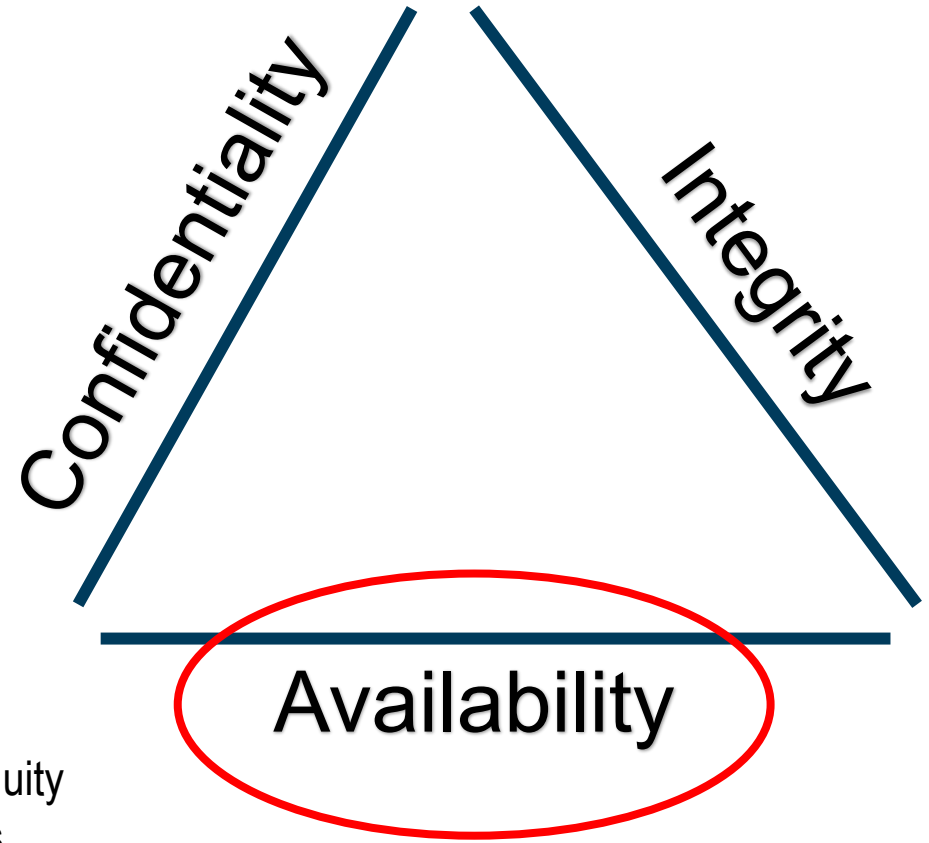
8 New laws or regulations

9 Fire

10 Supply chain disruption

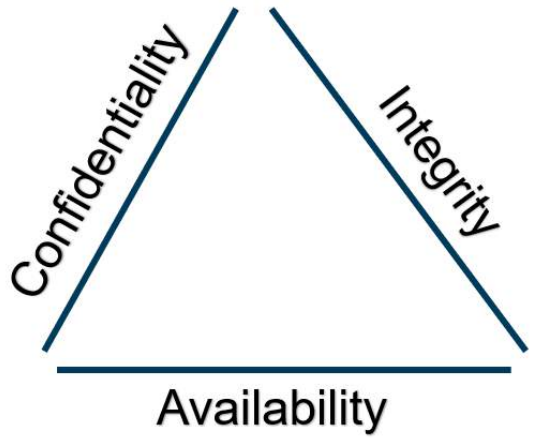
Information Security

- This model (CIA Triad or AIC Triad) is designed to guide policies for information security within an organization.



Don't Buy The Hype: High Availability is not a replacement for continuity planning. High Availability is about the Information Systems, Business Continuity is about the business processes.

CIA Triad
continued…



- ✓**Confidentiality**
  - Privacy
  - Encryption
  - Access Controls
  - Verification

Confidentiality prevents unauthorized disclosure of information.

- ✓**Integrity**
  - Consistency
  - Accuracy

Integrity assures that the data cannot be modified in an unauthorized manner.

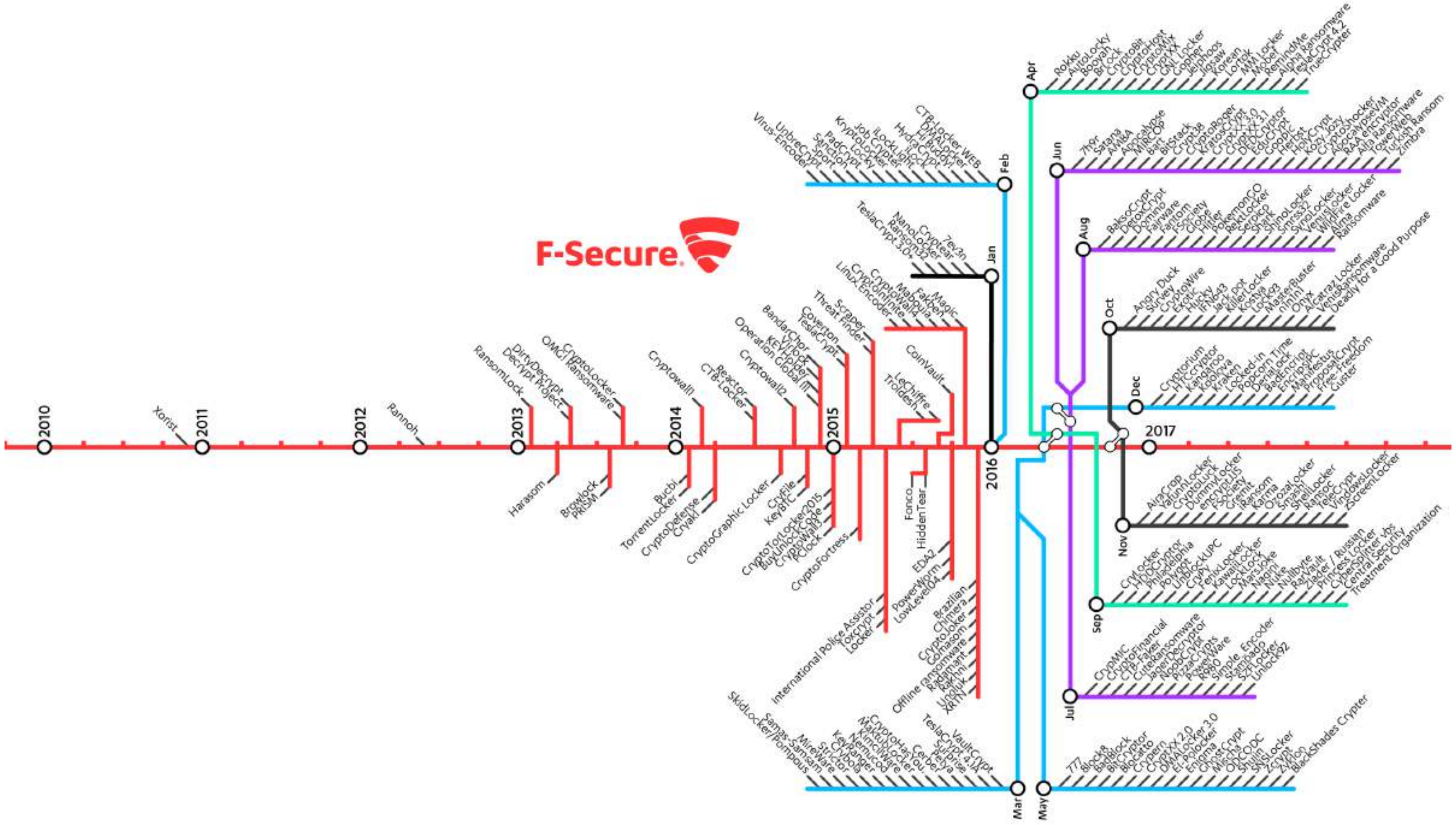
- ✓**Availability**
  - Redundancy
  - Bandwidth

Information should be readily available for authorized users.

WHY?! (Ransomware)

“Where’s my data and why can’t I access it?”

Image Courtesy of Sean Sullivan (FSecure)



BACKUPS

Terminology

Making sense of the technical jargon

- **Disaster Recovery (DR)** – A term that usually refers to the technology involved with a company. It would include the computer systems, communication, data network, etc.
- **Business Continuity Management (BC/BCM)** – A term that encompasses the whole operation including disaster recovery. Where disaster recovery is the technical aspect of the operation, business continuity relates to the operational side, people and processes. Includes 3 key elements:
  - **Resilience:** Creating (critical) business functions and supporting infrastructure that are well designed.
  - **Recovery:** Arrangements are made to recover or restore critical and less critical business functions.
  - **Contingency:** Establishing a generalized capability and readiness to effectively handle whatever occurs.

Terminology

Making sense of the technical jargon

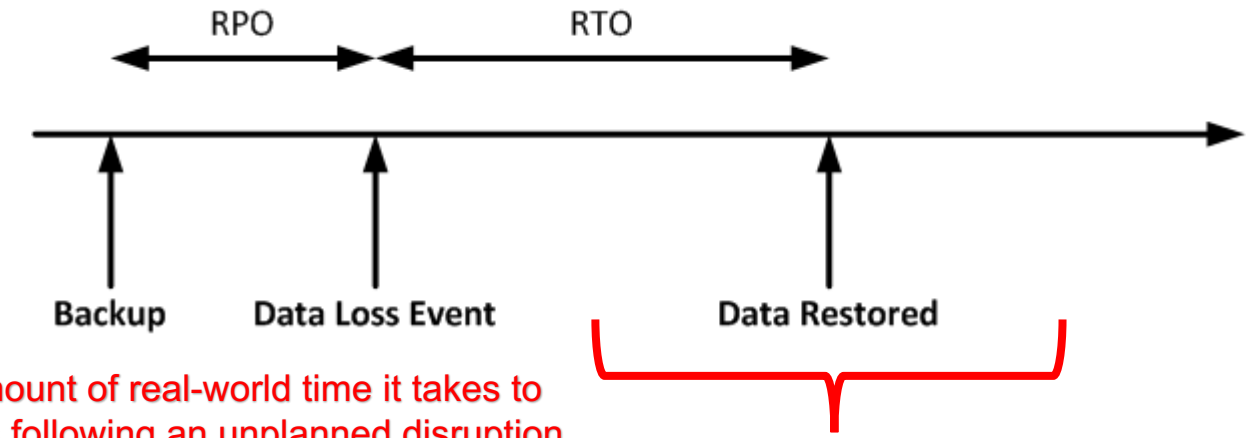
- **Risk Management** – A term that refers to the identification, assessment and prioritization of risks followed by coordinating resources to minimize, monitor and control the probability and/or impact of unfortunate events.
  - **Avoidance** – Is the practice of coming up with alternatives so that the risk in question is not realized.
  - **Transfer** – Is the practice of passing on the risk in question to another entity, such as an insurance company.
  - **Mitigation** – Is the practice of the elimination of or the significant decrease in the level of risk presented.
  - **Acceptance** – Is the practice of accepting certain risk(s), typically based on a business decision that may weigh the cost vs. benefit.

Terminology

Making sense of the technical jargon

- **Recovery Point Objective (RPO)** – The target set for the status and availability of data (electronic and paper) at the start of a recovery process in a known, valid state and can safely be restored from.

- **Recovery Time Objective (RTO)** – The target time for resuming the delivery of a product or service to an acceptable level following its disruption.



Recovery Time Actual (RTA) - The amount of real-world time it takes to recover systems and business processes following an unplanned disruption.

Terminology

Making sense of the technical jargon

- **Mean Time To Recovery/Repair (MTTR)** – A basic measure of the maintainability of repairable items. It represents the average time required to repair or recover a failed component, device or process.

- **Maximum Tolerable Downtime (MTD)** – A term that specifies the maximum period of time that a given business process can be inoperative before the organization's survival is at risk.
  - In the previous example it is the amount of time from the disaster until critical business operations resume. It could also be determined from the last successful backup.

Strategies

Understanding the options helps you get a ‘foot in the door’

- **Cold Site:** A cold site is the least expensive type of backup site for an organization to operate. It does not include backed up copies of data and information from the original location, nor does it include hardware already set up.

- **Hot Site:** A hot site is a duplicate of the original site of the organization, usually with full computer systems as well as near-complete backups of data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software.

- **Warm Site:** A warm site is a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites might have backups on hand, but they may not be complete or recent.

Strategies

Understanding the options helps you get a ‘foot in the door’

- **Service Bureau:** A company to partner with that specializes in disaster recovery services and can provide guidance and resources on-demand to accelerate recovery during an event. Companies can offer physical and/or virtual assistance and could be considered DRaaS (Disaster Recovery as a Service). These companies typically provide a wide range of support before, during and after an event.
  - Facilities such as mobile sites or alternative office space.
  - Power and data communications along with networking equipment.
  - Workstations, servers and printers (preconfigured or ‘bare bones’).
  - Checklists and periodic check-ins to make sure plan is still accurate.

Processes

Understanding the technology behind the business

Servers (Physical vs. Virtual)

- Physical Server recovery is typically longer and more expensive than its virtual counterparts.
- Virtual Servers have more options when it comes to recovery and even normal operations. There are also cost savings from virtualizing IT infrastructure and simplicity in the backup and restoration process.
- Services such as IaaS (Infrastructure as a Service) or PaaS (Platform as a Service) offerings allow you to build datacenters in the cloud and/or combine on-premise infrastructure to increase resiliency.

Processes

Understanding the technology behind the business

Data Storage and Backups

- Make sure critical system data is backed up based on the RPO gathered through this exercise. It's important to make sure that the backup method is appropriate for the data type being protected.

- Backup data is moving (has moved) from traditional tape/disk based to SAN or virtual SAN architectures even hosted cloud service providers: Google Drive, Microsoft OneDrive, Microsoft Azure, Amazon AWS, etc.

- You can leverage storage on-premise, off-site and in the cloud to build a stronger backup strategy.
  - **PLEASE NOTE:** It's important to always encrypt sensitive data and ensure that the privacy settings on storage are tied down based on 'least privilege'.

Processes

Understanding the technology behind the business

Core Business Functions (Email, Telephone and Fax)

- Consider using web-based email services in addition to or in replacement of on-premise solutions.
  - High availability options exist that allow companies to quickly leverage alternate data processing resources in the event of a failure.
- Unified Communications are VoIP solutions that offer flexibility with business telephony and have an edge over on-premise systems that may require servers, software and staff to rebuild.
  - ‘Softphones’ are easy to use and can replace the need for handsets to be provisioned.
  - Many solutions also offer Fax alternatives and advanced call routing and recovery options.

Processes

Understanding the technology behind the business

Software (Subscription vs. Purchased)

- Software companies are switching from the traditional (boxed) model to a subscription service such as Office 365.
  - Many times they also offer web versions that do not require any software to be installed on the local machine; this lowers the MTTR.
- Depending upon the software necessary for your company to operate SaaS (Software as a Service) solutions may provide a cost savings.
- Remember to store critical software somewhere accessible.
  - For example: If you need specialized software to start the restoration process, make sure this software, licenses, encryption keys, usernames, etc. are readily accessible by the necessary individual(s).

Establishing a Framework

Step-by-Step guide to create an actionable plan

- Due to the high cost of ineffective plans, information about planning and crisis management processes are readily available.
  - ISO 22301
  - NIST SP 800-34
- Planning provides procedures for how employees and employers will stay in touch and keep doing their jobs in the event of a disaster or emergency.
- IT should be involved in every step of the process.
  - Many times IT understands the interdependencies of connected system that make business processes run, but they do not always know why or what departments need.

Establishing a Framework

Step-by-Step guide to create an actionable plan

- Before starting it is critical to have senior management's support to allocate sufficient resources and personnel to the project.

- BCM can be used by companies to differentiate resilience to potential or existing customers
  - Process analysis and monitoring can expose business inefficiencies.
  - Retaining customers following a disaster is less expensive than acquiring new customers.
  - Successful experiences can build morale among employees which prevents excessive turnover.

Step 1

Initial Assessment and Objective Setting

- Initiation and Management Involvement
  - Set up an executive level sponsor to provide awareness to the organization. They must sell the importance of the program to the executive team.
- Determine Subject Matter Experts (SMEs) in all aspects of your business operations.
  - Identify the team in charge of the planning and overall success of the process.
- Draft a plan that outlines the objectives of the organization.
  - It should include the scope and timeline of deliverables.
- Develop a contingency planning policy statement.
  - A formal policy provides the authority and guidance necessary to develop an effective plan.

Step 2

Critical Process Identification

- Identify the organization's most critical business functions
  - Prioritize these based on criticality to the business, maximum tolerable downtime and the impact to the organization. You should assign team members responsible for their restoration.
- Document critical business equipment and software.
  - Compile all documentation necessary to start your business over again in the event of a fire or other disaster that destroys your critical on-site documentation. (i.e. encrypted USB devices or cloud storage, etc.)
- Document external contacts such as vendors, contractors and customers.
  - This includes, attorneys, bankers, IT consultants, utilities, etc.
- Pinpoint key resources and tools that enable processes to be executed.
  - Facilities, specialized hardware, etc.
  - People and Skill Sets (identify who can telecommute in the event that business operations cannot continue at the regular location)

Step 2

Critical Process Identification

- Identify the business objectives and processes.
- Process owners should identify:
  - Performance Metrics or Key Performance Indicators (KPIs)
  - Contracts with external parties
  - Regulatory and/or legal requirements (SLAs, SLOs, etc.)
- Management should establish recovery priorities for business processes that identify the following:

• **Essential Personnel**	• **Facilities**
• **Succession Plans**	• **Communications**
• **Technologies**	• **Vital Records and Data**

Step 3

Conducting the Business Impact Analysis

- The Business Impact Analysis (BIA) will help the company decide what needs to be recovered, and how quickly. Mission functions are typically designated as the following to help determine appropriate prioritization.
  - Critical, Essential, Supporting and Non-Essential.
  - Determine the impact of a system disruption to those critical systems.
- Identify resource requirements to resume critical processes quickly.
  - Is there specialized equipment, hardware, software or knowledge required.
- Identify recovery priorities for system resources.
  - System resources can be linked more clearly to critical business processes and functions.
  - Recovery in the proper sequence is important!

Step 3

Business Impact Analysis

- Identify the Quantitative (measurable) and Qualitative (usually reputational) impact that each critical process has to the business.
- Identify the following impacts to specific business processes and corporate functions when a disaster occurs:
  - Human Resources
  - Reputation
  - Physical Assets
  - Relationships (customers/vendors)
- Determine what is necessary to restore critical operations. Prioritize the need to restore each item after an event.
  - Identify a Recovery Time Objective for each process identified in Step 2.

Step 3

Business Impact Analysis

- Results of the BIA contain:
  - Critical departments and required resources
  - Threats and risks to the business
  - Impact company can handle dealing with each risk
  - Outage time that would not be critical
  - Recovery alternatives
  - Priority for recovery based on relationships
- These results should be documented and used to create balanced recovery plans in the next step.
  - Encourage your employees to keep instruction manuals and procedures of their own.

Step 4

Continuity Response Approaches (Preparation)

- Consider adopting policies that prevent a set amount of executives, managers and/or other critical personnel from traveling together.
- Contact lists are created and maintained for each employee who is required to restore a critical business process.
- Work with IT managers to ensure that valid backups exist and are tested.
  - Be sure to evaluate and prioritize the recovery time needs of each critical system.
- Conduct a cost-benefit analysis to better identify the proper balance between recovery time objective and the cost of recovering data and restoring systems within those timeframes.
- Identify alternate vendors in the event of a disaster that prevents one or more vendors from operating.

Step 4

Continuity Response Approaches (Crisis Management)

- Determine who should be part of this team.
  - i.e. Quick effective and decisive people that know the interdependencies within an organization's processes are prime candidates.
  - Create a Crisis Communications Planning Checklist.
- Provide a highly detailed account of how critical processes will be restored.
- Provide a detailed plan for notifying and updating the following audiences about the event's impact on the business.
  - Employees
  - Customers
  - Vendors
  - Media

Step 5

Plan Implementation and Testing

- Types of Testing Exercises
  - Checklist
  - Structured Walkthrough (Role-Playing)
  - Simulation
  - Parallel
  - Full Interruption (Mock Disaster Test)
    - The goal is to simultaneously test as many components as possible. This type of test is likely to be costly and could disrupt normal operations.

Step 5

Plan Implementation and Testing

- Frequent testing of the plan is crucial to ensure that employees are familiar with the steps to take in the event of a disaster.
  - Use this time to identify gaps and inconsistences in the plan.
  - Test business continuity plans at least once a year.
  - When conducting tests, involve operational and functional employees as well as managers.
  - Ensure time sensitive processes are recovered to a minimal acceptable level.

- Testing identifies limitations of emergency plans, business continuity plans and disaster recovery plans.
  - Most organizations change frequently, even mature business continuity plans may be inappropriate in a given situation or at a given time.

Step 6

Monitoring, Validating and Improving (Maintenance)

- As changes in the business occur, be sure to adjust business impact analysis and business continuity plans accordingly.
  - It is very important to Test, Train and Maintain.

- Identify weaknesses and gaps uncovered during the test exercises.
  - Some adjustments take time and may require additional resources.
  - Develop a timeline to eliminate or remediate weaknesses and report on the outcome to key managers.

Creating a ‘Run Book’

- A ‘run book’ refers to a set of defined procedures developed by the system administrator or other IT professional for maintaining the everyday routine as well as the exceptional operations of the network and systems.

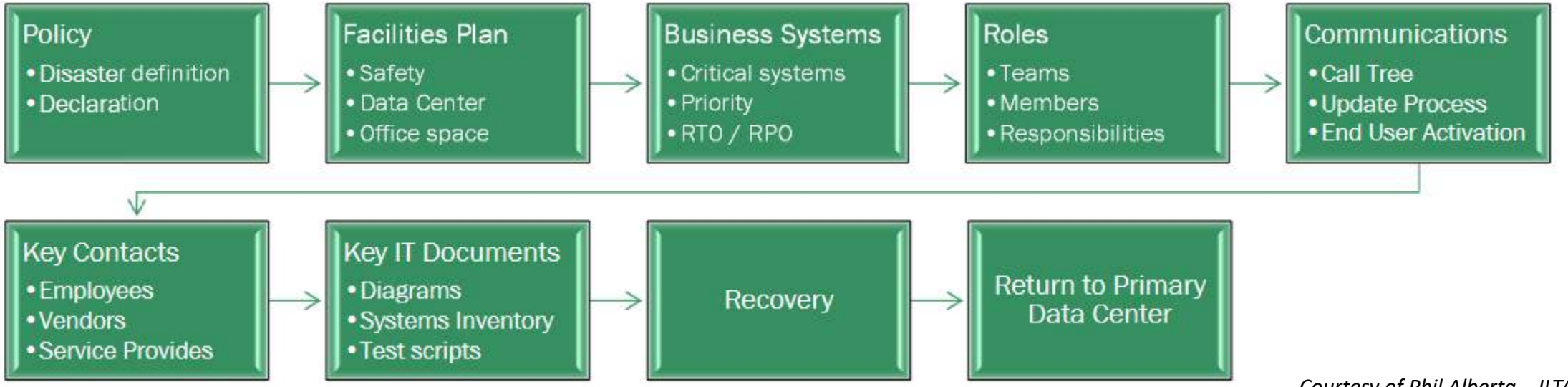
- This ‘run book’ should contain all the information staff would need to perform daily operations as well as information on dealing with problems that arise.

- You will be able to delegate tasks and onboard employees more effectively if you have good documentation to train them with.

- Use the KISS Principle when beginning to document, or compile existing documentation. It’s important to use a Table of Contents for organization.

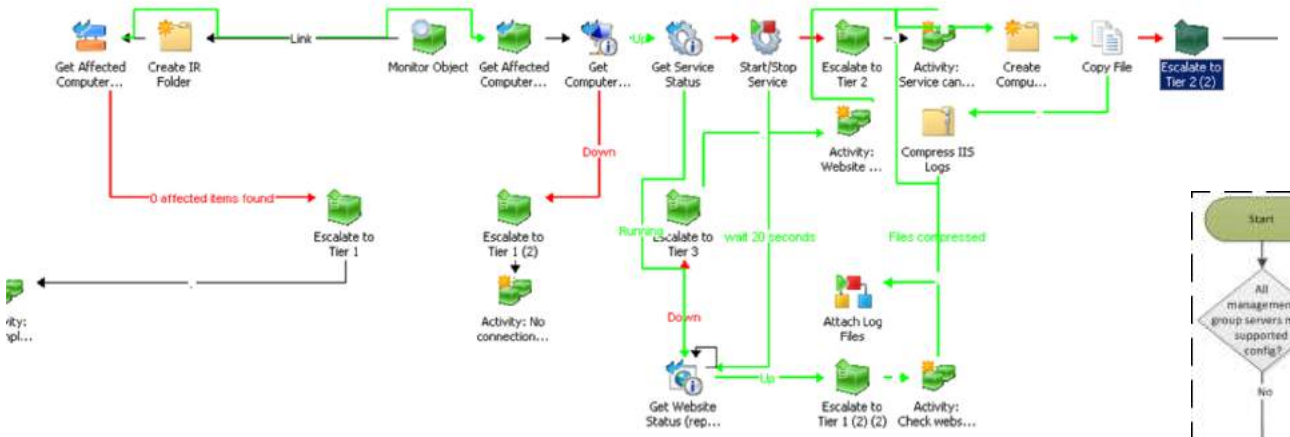
Creating a ‘Run Book’

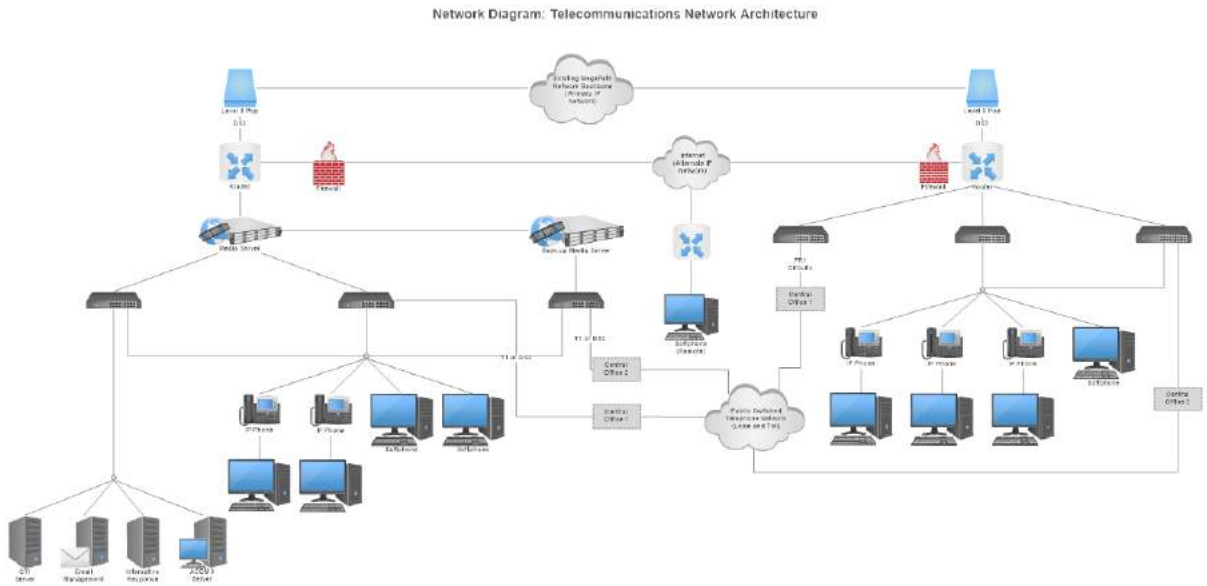
- Identify an owner, someone (or a group) responsible for maintaining the documentation and updating it as part of a change management process.
- Set clear expectations of what IS and IS NOT contained or possible with the documentation.

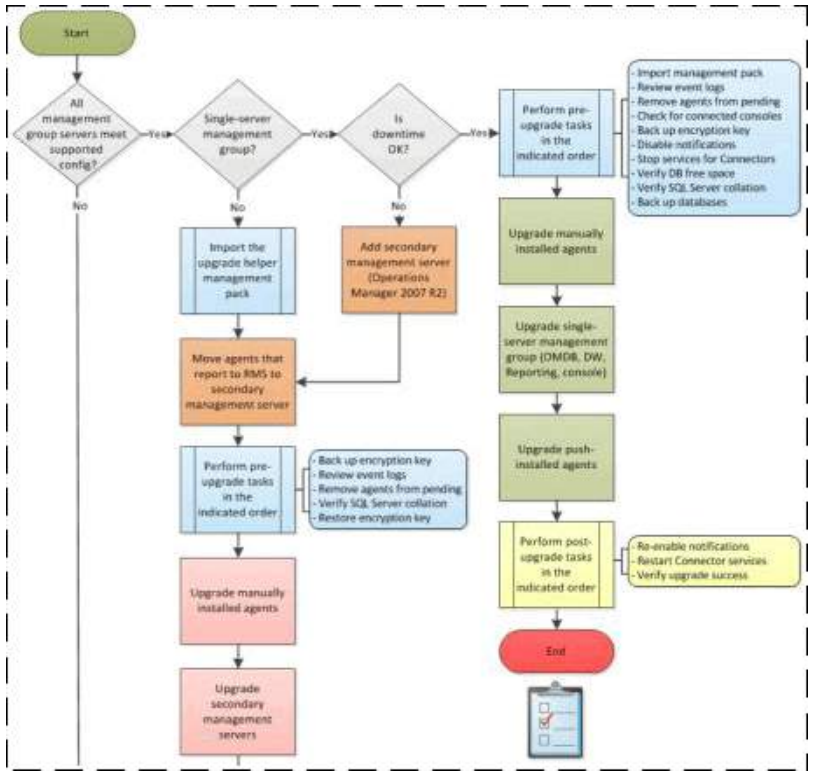


Courtesy of Phil Alberta – ILTACON 2017

Creating a ‘Run Book’







Creating a ‘Run Book’

- Operational run books should contain scenarios and use cases along with detailed instructions and procedures to restore normal operations.
- A comprehensive run book should contain information such as:
  - Contact Information for employees, vendors and consultants
  - Infrastructure Overview (Data Center, Network Layout, Physical Access, Facilities)
  - Order of Restoration (Start up and shut down procedures)
  - System Configuration (Baselines)
  - Backup Configuration
  - Monitors (Alerts or checks on production system)
  - Roles and Responsibilities
  - Data Restoration Processes

Always keep up-to-date documentation and revision control

Wrapping Up

- The documentation you create through this process should be in multiple locations, secured, but easily accessed with the right set of credentials, knowledge, etc. during an unexpected event.
  - Consider leveraging cloud platforms for availability and recovery of important business process documentation.
  - Each department or business group could have its own plan that rolls up into the overall Business Continuity Plan for your organization.

Additional Resources and References

- The Business Continuity Institute
  - www.thebci.org
- Disaster Recovery Journal
  - www.drj.com
- The Risk Management Society (RIMS)
  - www.rims.org
- Disaster Recovery Institute
  - https://drii.org

- ISO 22301
  - https://www.bsigroup.com/globalassets/Documents/iso-22301/resources/iso-22301-implementation-guide-2016.pdf
- NIST SP 800-34
  - https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf

Remember the key to DR and BC Plans is finding alternative ways to process business transactions

“An ounce of prevention is worth a pound of cure”

-Benjamin Franklin

Questions?

BIG UNIVERSITY 2018

Owner / Principle Track

SESSION 2

"Sucker Punches"

Erich Kron (KnowBe4)

Erich Kron

Security Awareness Advocate

About Erich Kron

- CISSP, CISSP-ISSAP, MCITP, ITIL v3, etc…
- Former Security Manager for the US Army 2nd Regional Cyber Center – Western Hemisphere
- Former Director of Member Relations and Services for $(ISC)^2$
- A veteran of IT and Security since the mid 1990's in manufacturing, healthcare and DoD environments

CISSP® Certified Information Systems Security Professional

CISSP® Certified Information Systems Security Professional

ISSAP® Architecture

Microsoft® CERTIFIED IT Professional

Over

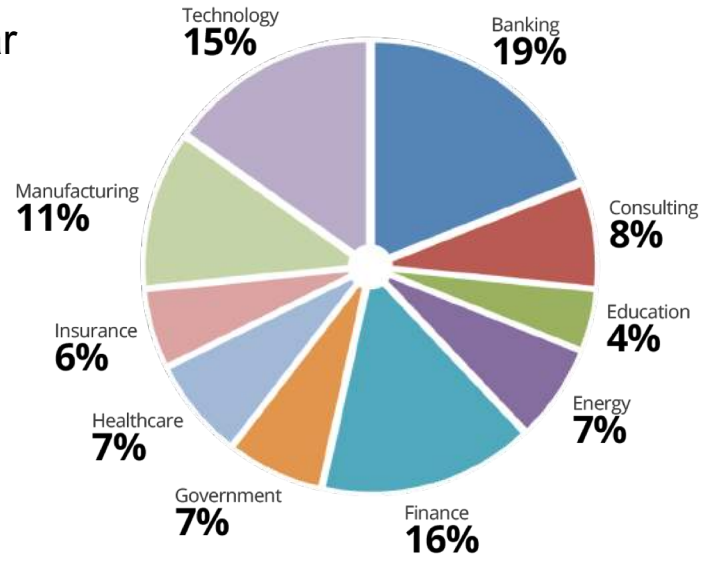
17,000

Customers

Inc. 5000

About Us

- The world's most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- Former Gartner Research Analyst, Perry Carpenter is our Chief Evangelist and Strategy Officer
- 200% growth year over year
- We help thousands of organizations manage the problem of social engineering



KnowBe4
Human error. Conquered.

Phishing: By The Numbers

KnowBe4
Human error. Conquered.

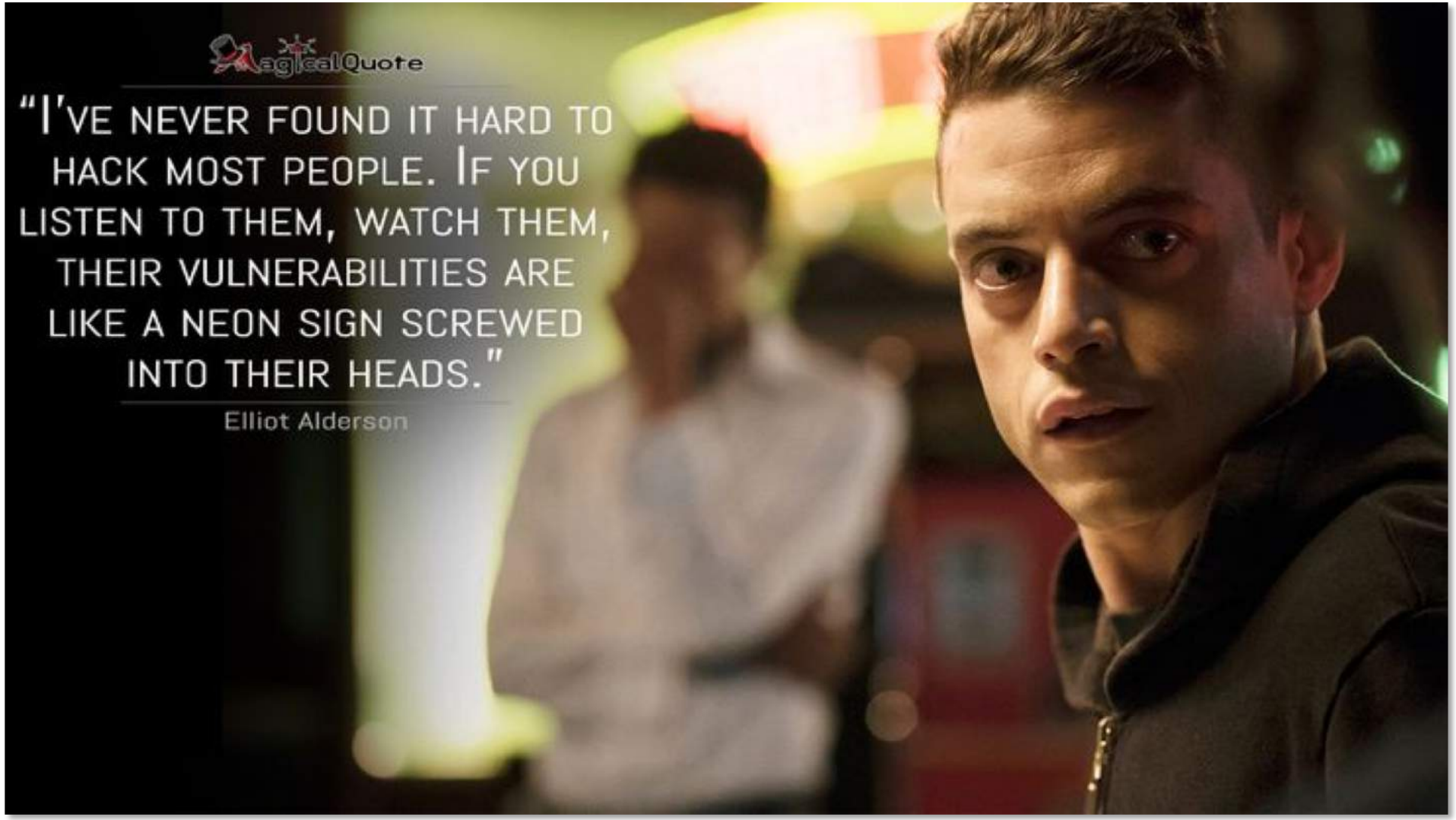
Employees Are the Last Line of Defense

- **91%** of successful data breaches started with a spear phishing attack
- **Ransomware** is predicted to exceed damages of $5 billion in 2017, and continues to grow
- **CEO fraud** (aka Business Email Compromise) estimated to exceed $9 billion in 2018
- **W-2 scams** social engineer Accounting/HR to send tax forms to the bad guys

The Costs of Breaches and Ransomware Attacks

- In 2017 Ransomware **grew 300%** over 2016
- Ransomware is predicted to exceed **damages of $11.5 billion** by 2019, and continues to grow
- Over 153,000 users were hit by **mobile ransomware** in 2016

Social Engineering



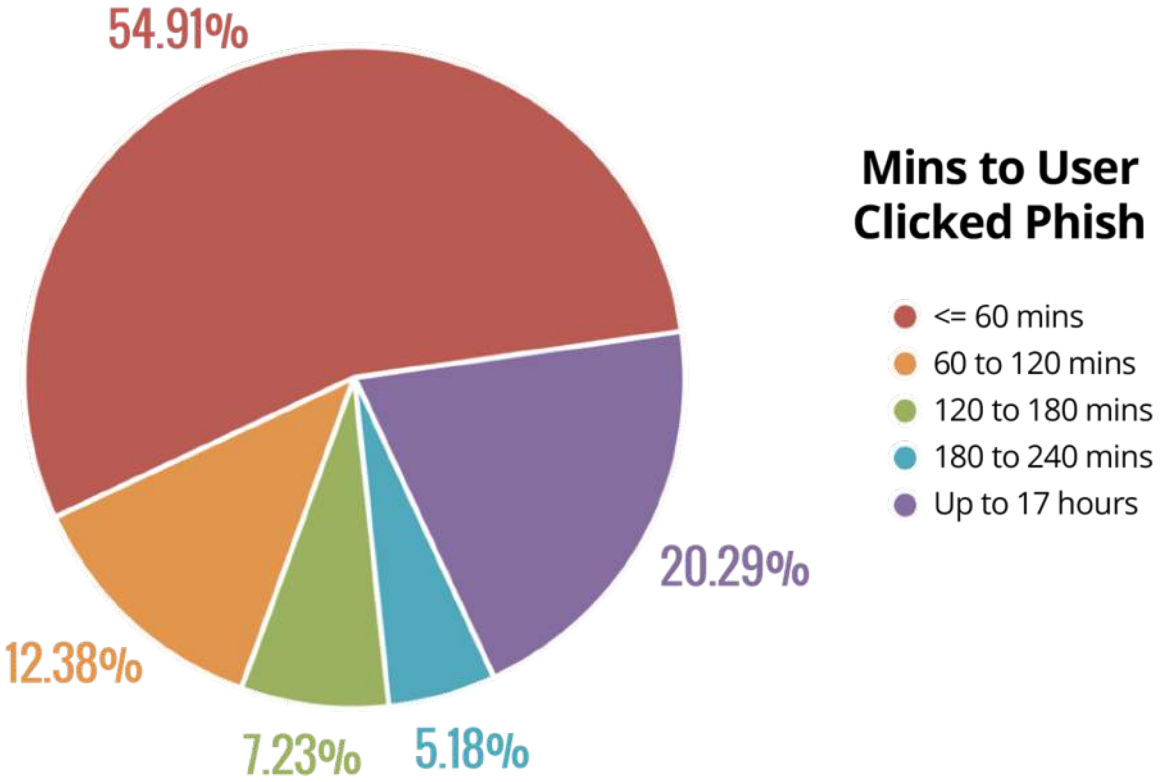
Recent studies show that over

54.9%

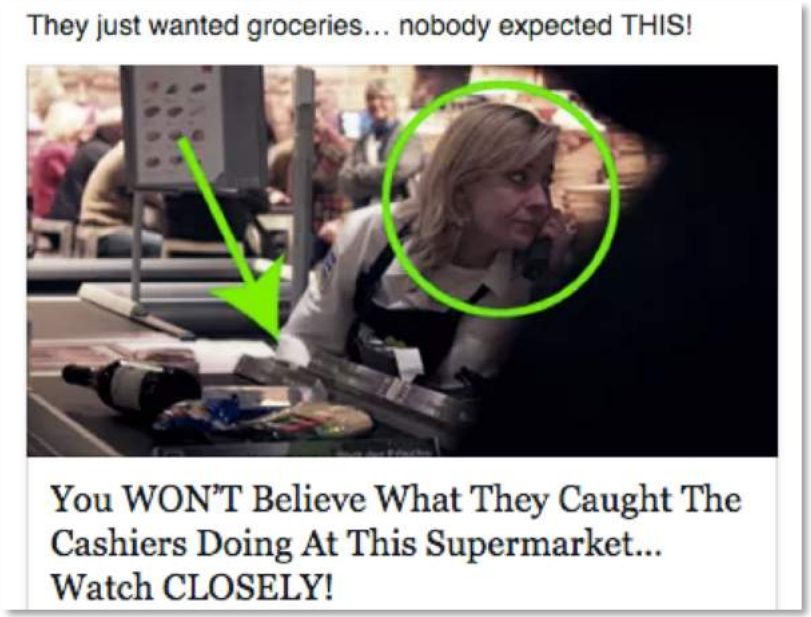
of users click on a phishing link
in under 60 minutes

KnowBe4
Human error. Conquered

When Do People Click On Phishing Links?



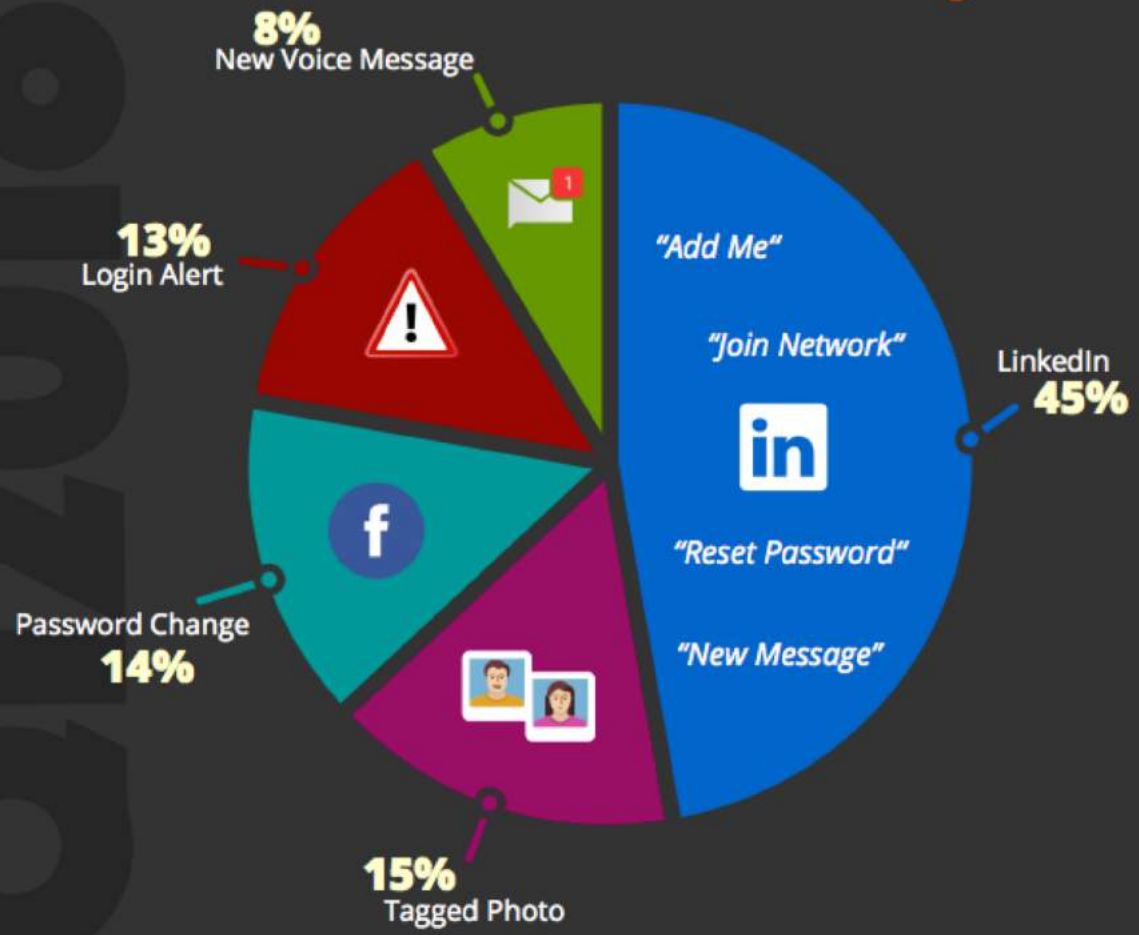
Clickbait: It's More Science Than You Think



- Leverages "pattern interruption" to create curiosity often based on the "information-gap" theory
- "Such information gaps produce the feeling of deprivation labeled curiosity. The curious individual is motivated to obtain the missing information to reduce or eliminate the feeling of deprivation." - George Loewenstein, Carnegie Mellon
- Also leverages outrage and anger, which drives us to take action

TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



TOP 10 GENERAL EMAIL SUBJECTS

A Delivery Attempt Was Made	21%
Change of Password Required Immediately	20%
W-2	13%
Company Policy Update for Fraternization	10%
UPS Label Delivery 1ZBE312TNY00015011	10%
Revised Vacation and Time Policy	8%
Staff Review 2017	7%
Urgent Press Release to All Staff	5%
Deactivation of (email) in Process	4%
Please Read: Important From HR	2%

KEY TAKEAWAY

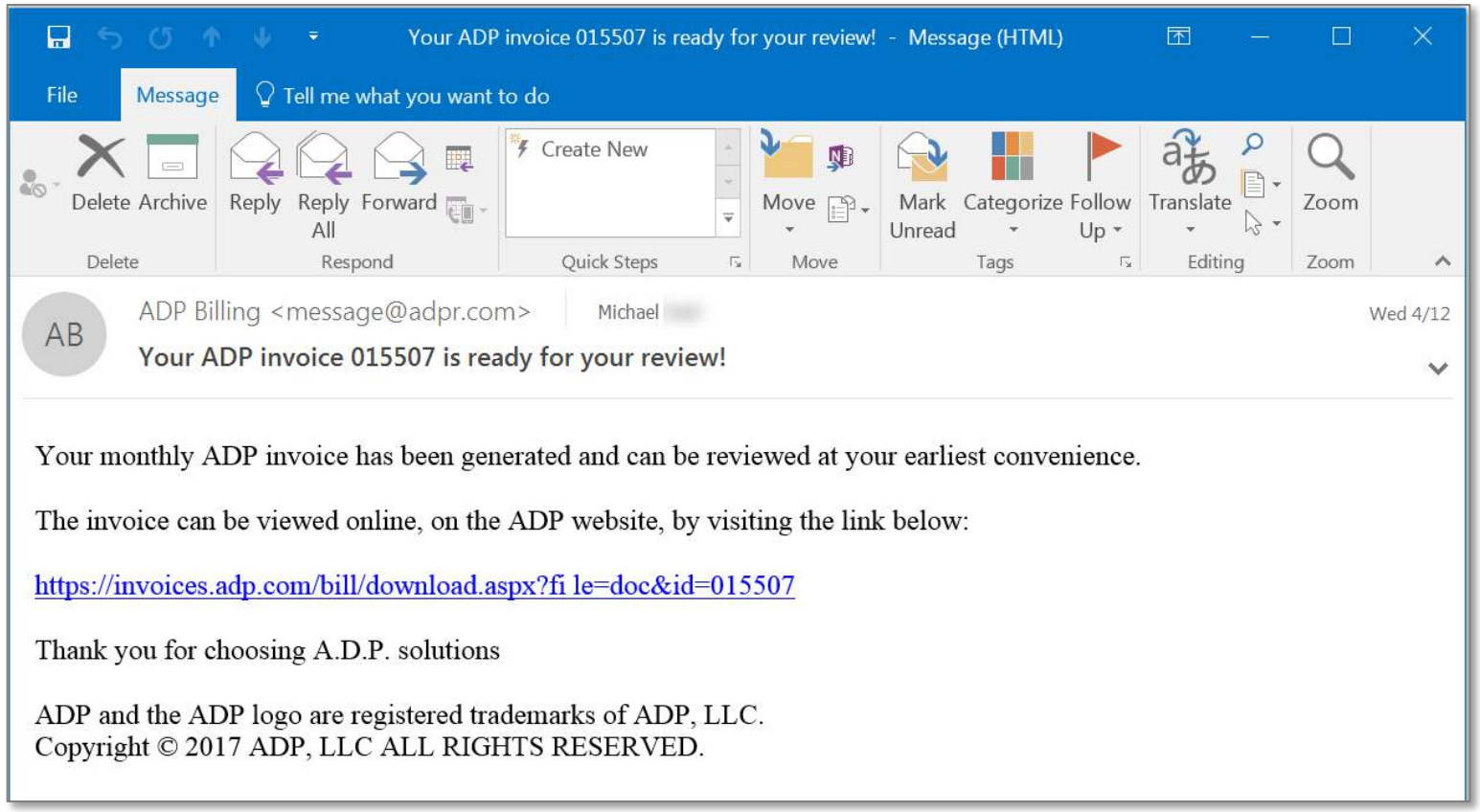
Email is an effective way to phish users when disguised as legitimate email. These methods allow attackers to craft and distribute enticing material for both random (general phish) and targeted (spear-phish) means, leveraging multiple psychological triggers and engaging in what amounts to a continuous maturity cycle.

COMMON *"IN THE WILD"* ATTACKS

- IT DESK: Security Alert Reported on Campus
- IT DESK: Campus Emergency Scare
- IT DESK: Security Concern on Campus Earlier
- Amazon: Billing Address Mismatch
- Password Review
- Urgent Security Event: Your account details were found online
- Wells Fargo: New device detected
- Microsoft: Updates to our terms of use
- GasBuddy: Major car recall announced today
- CNN: Facebook-Cambridge Analytica Apology Tour

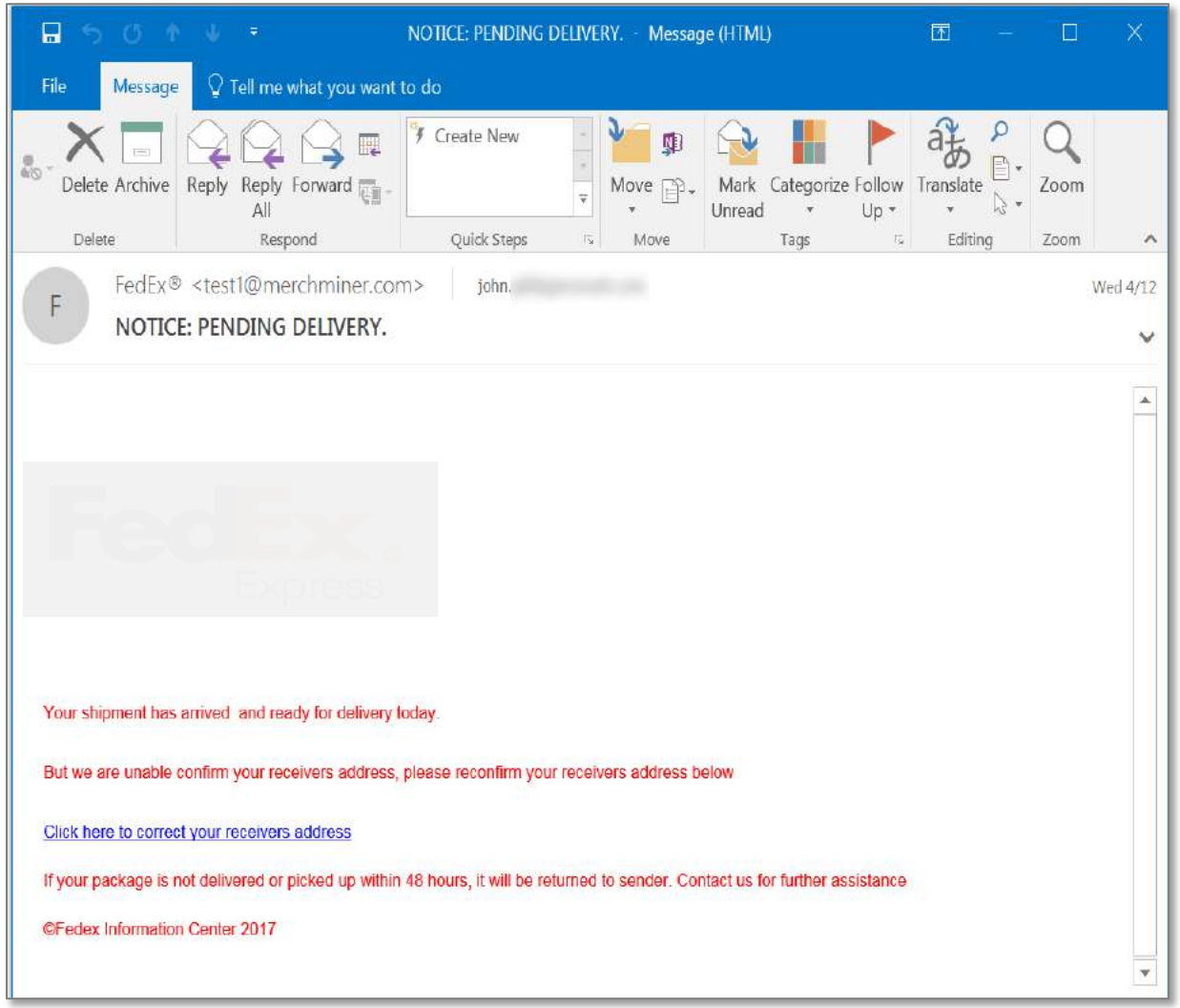
The Invoice/P.O. Phish

- The most common phishing genre in the emails reported to us via the Phish Alert Button (PAB)
- This type of phish easily blends into the deluge of emails that employees in many positions deal with on a daily basis.



The Package or Parcel Delivery Phish

- Companies and organizations in the business of delivering packages and parcels now email customers and users on a daily basis.
- Once again, the bad guys regularly seek to capitalize and exploit this kind of business-to-business communication by crafting phishing emails that mimic those sent by recognized organizations like USPS, UPS, FedEx, and DHL.

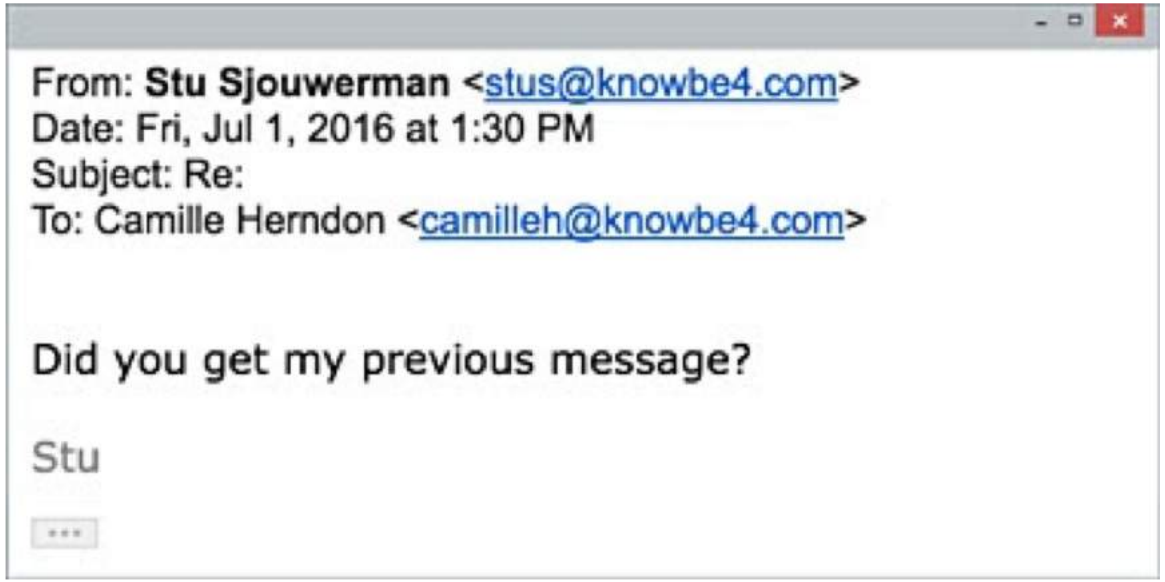


CEO Fraud: Protecting The Targets

KnowBe4
Human error. Conquered.

How CEO Fraud Plays Out

- KnowBe4 had just hired a new controller. Part of the onboarding process is updating LinkedIn
- A few weeks later, she receives this email, but the email headers proved it's not from Stu
- This was a real CEO Fraud attempt, just a few weeks after she had updated her LinkedIn account



Two Unnamed US Companies Falls Victim to $100 Million CEO Email Fraud

- This scam only surfaced as the U.S. government filed a civil forfeiture lawsuit in federal court in Manhattan seeking to recover tens of millions held in at least 20 bank accounts around the world.

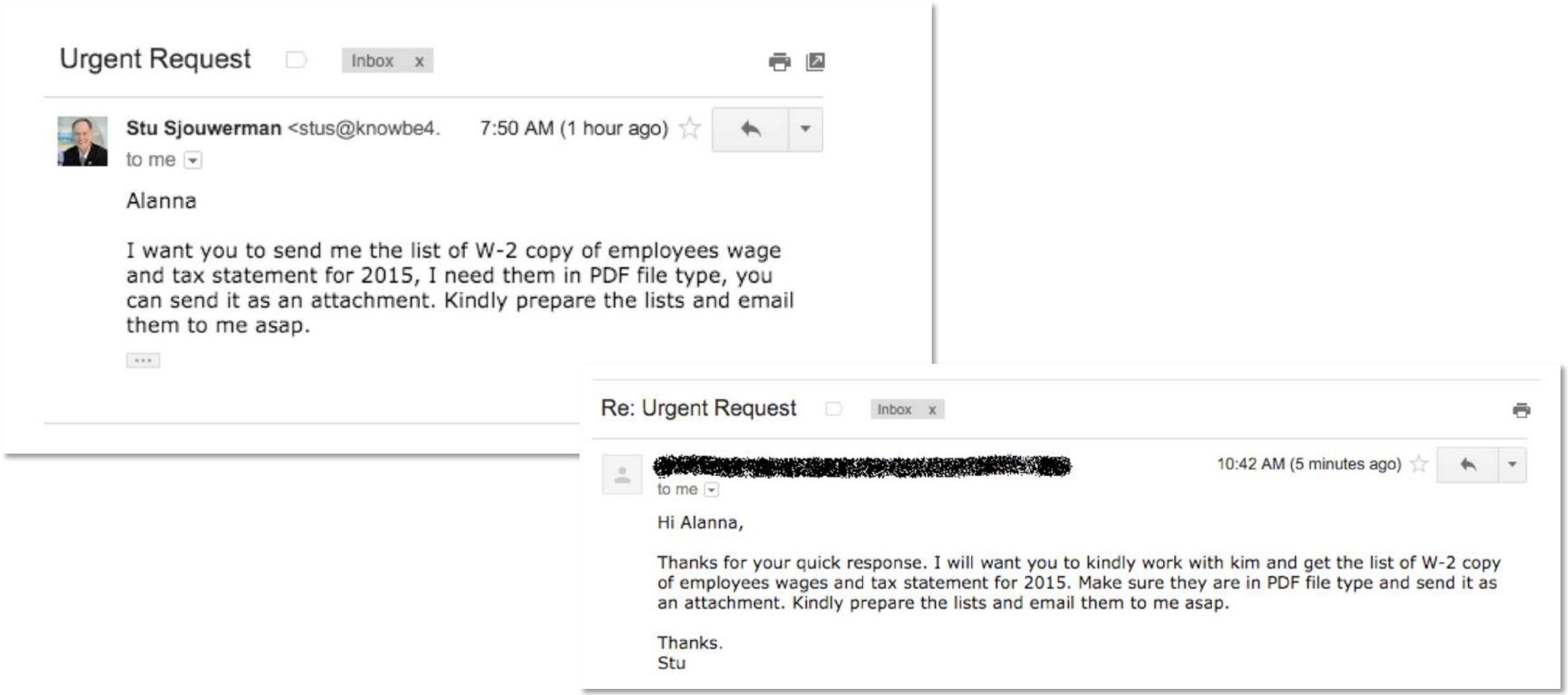
- The scammer, a 48-year old Lithuanian managed to trick two American technology companies into wiring him **$100 million**.

- What makes this remarkable is the amount of money he managed to score and the industry from which he stole it. The indictment specifically describes the companies in vague terms, but Apple, Cisco, HP and Facebook come to mind.

$44 Million in a Single CEO Fraud Attack

- Leoni AG fell victim to a classic CEO Fraud attack that has cost the company a whopping **44 million dollars**.
- Attackers crafted emails to appear like legitimate payment requests from the head office in Germany and sent them to a subsidiary of Leoni in Bistrita, Romania.
- The scammers had extensive knowledge about the internal procedures for approving and processing transfers, meaning the network had likely been penetrated months earlier.

Urgent Request for W-2s



Urgent Request

Inbox x

Stu Sjouwerman <stus@knowbe4. 7:50 AM (1 hour ago)

to me

Alanna

I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.

Re: Urgent Request

Inbox x

[redacted] 10:42 AM (5 minutes ago)

to me

Hi Alanna,

Thanks for your quick response. I will want you to kindly work with kim and get the list of W-2 copy of employees wages and tax statement for 2015. Make sure they are in PDF file type and send it as an attachment. Kindly prepare the lists and email them to me asap.

Thanks.
Stu

My W-2 Fraud Story

- 250 employee company
- Not really well known or heavily marketed
- President was traveling, the email requested W-2s
- Signature was correct, probably from his out-of-office reply
- HR person felt something was fishy (phishy?) and gave me a call

Ransomware: Know The Enemy

KnowBe4
Human error. Conquered.

RaaS: Ransomware as a Service

- This is designed to let people that are not technical set up attacks
- Different ways of doing this, for example, Philadelphia is $400, Dot is free with a 50/50 split of profits, Saturn and Cerber RaaS models are free with a 70/30 affiliate/malware developer split

Infected Apps: LeakerLocker

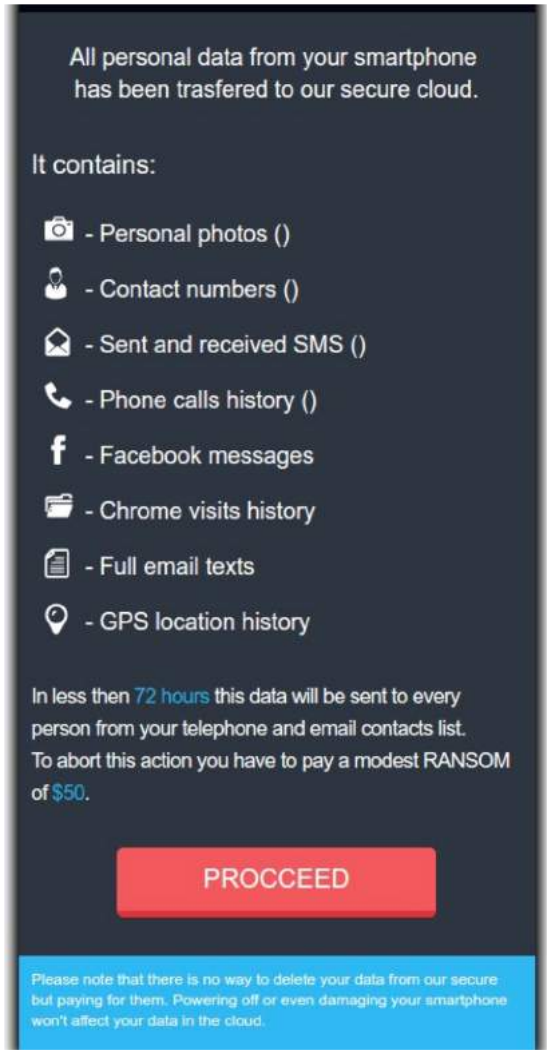
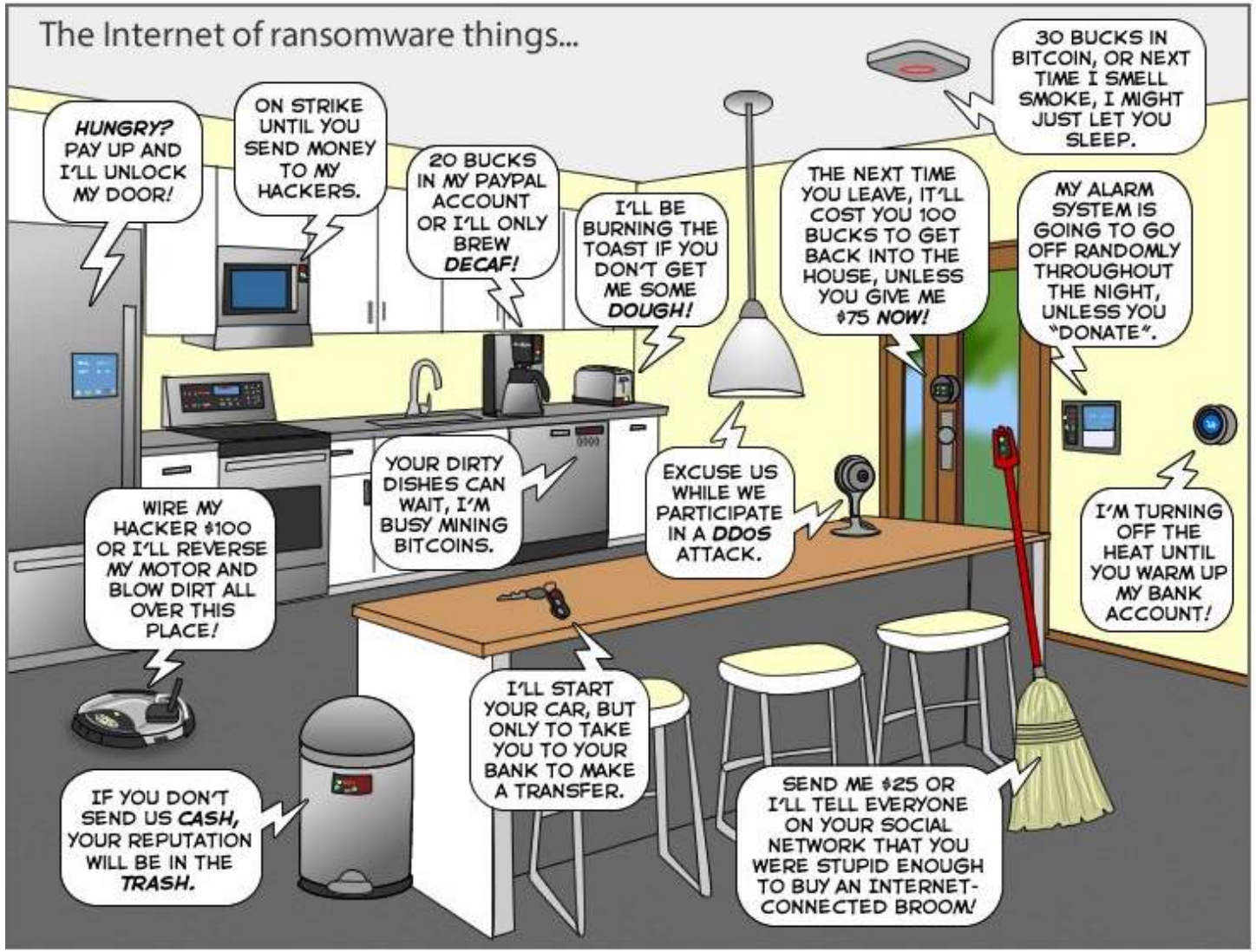


Image Source: bleepingcomputer.com/

- This is Android Doxware
- Does not root, relies on permissions granted during install and locks the screen
- Found in"Wallpapers Blur HD" and "Booster & Cleaner Pro" apps
- Both were **part of a rewards program** that paid to install an app

The Future of Ransomware



Arm Employees For Battle

KnowBe4
Human error. Conquered.

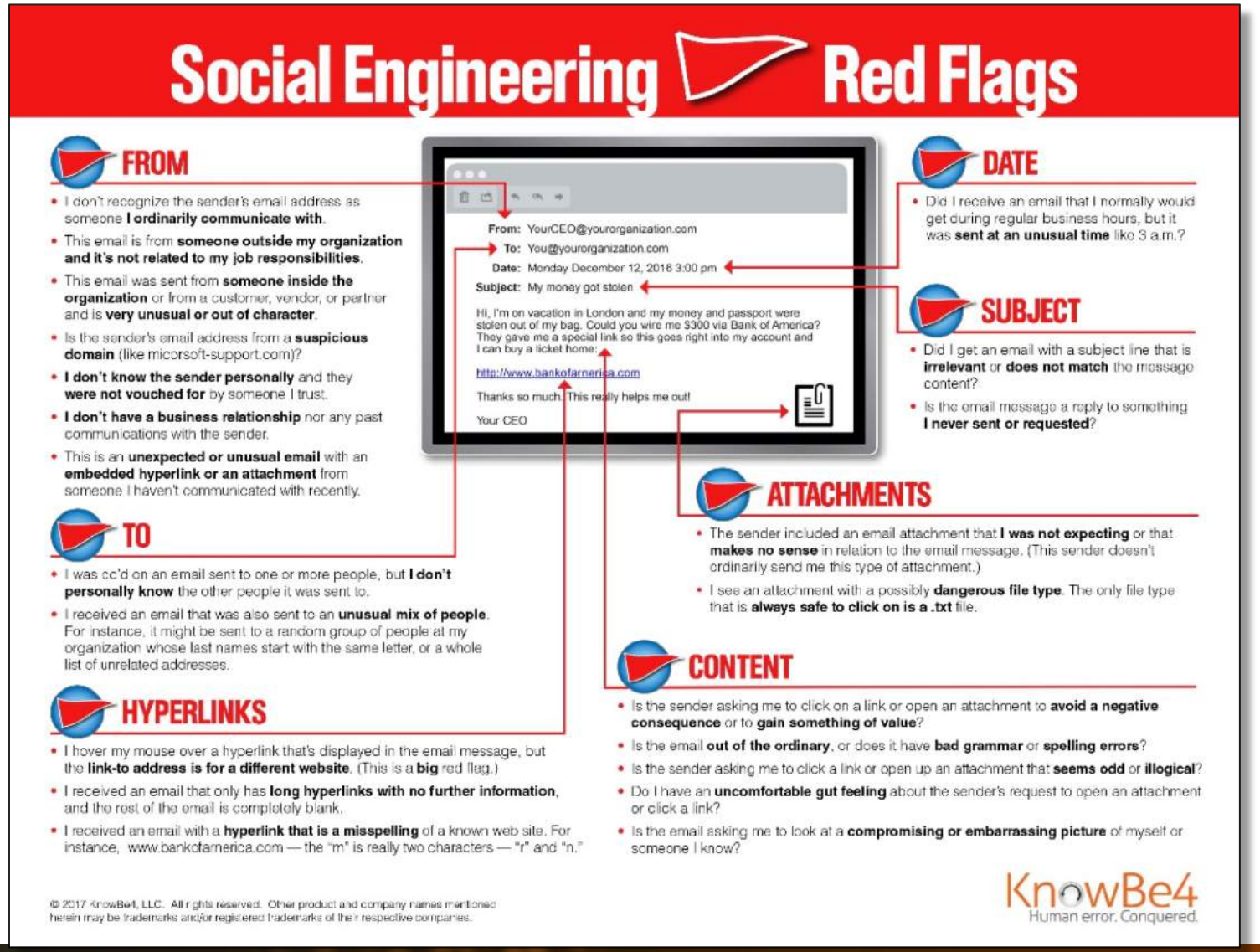
Comprehensive Programs Work

- Most security awareness programs are still too superficial and done for compliance reasons
- What is missing is the correct estimation of the adversary being faced and the degree of commitment an organization has to have to stave of attacks

Develop a Coordinated Campaign

- Training on its own, typically once a year, isn't enough
- Simulated phishing of groups of employees on its own doesn't work
- But together, they can be combined to greatly increase effectiveness

How can we protect our current businesses?



Training: How To Do It Right

KnowBe4
Human error. Conquered.

The KnowBe4 Security Awareness Program WORKS

Baseline Testing
We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

Phish Like the Bad Guys

Conduct “Full Random” Phishing Attacks

- Prairie dogging is when an employee notices a simulated phishing email and warns the others in the office about it. Or employees get used to the simulated campaigns, and learn to watch out for them
- The way to guard against this is to use what are termed full random simulated phishing attacks
- This entails the selection of random message delivery, and random phishing templates to gain a more accurate estimate of an organization’s likelihood to fall victim to phishing

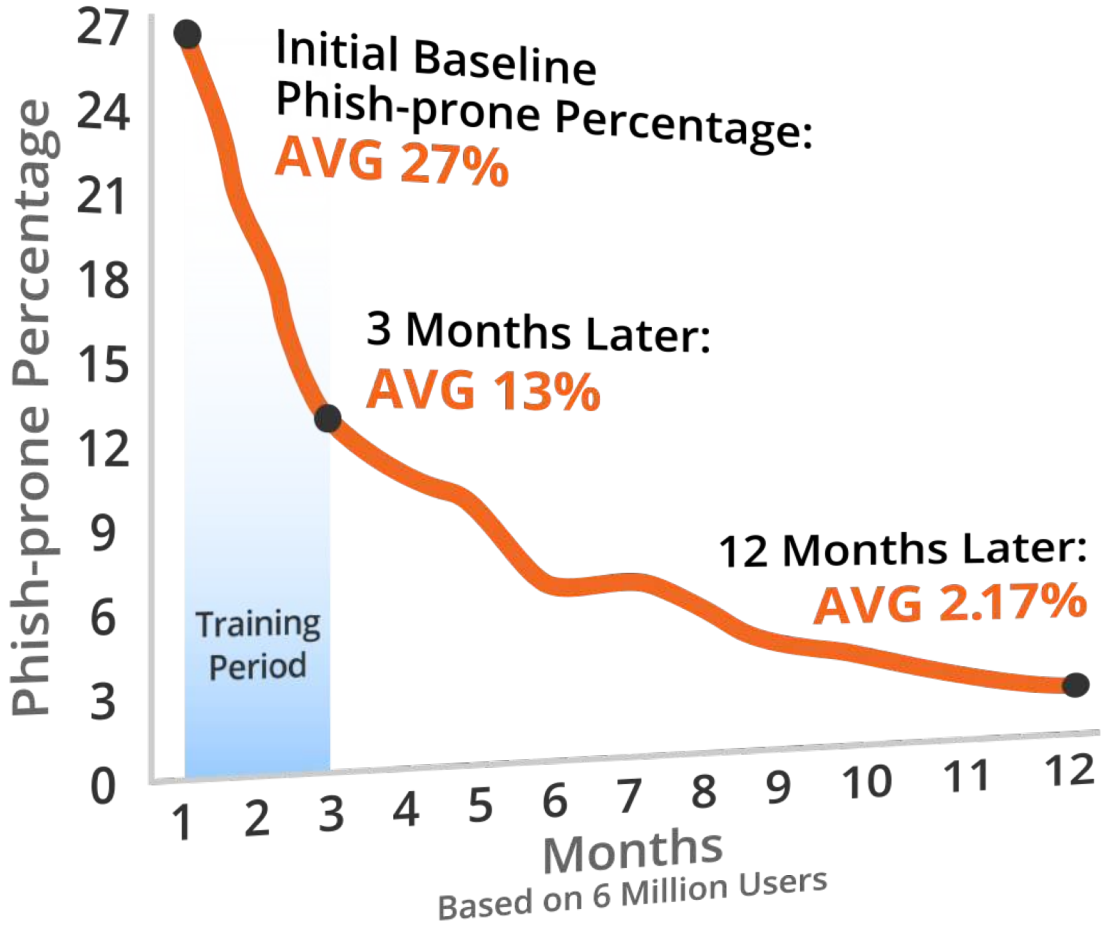
Phish Like the Bad Guys

Personalize Emails

- Just adding an employee's first name isn't enough. Personalization must be taken further
- For example, add an attachment named, "Q4 Payroll" and make it look like it's sent to them accidentally by referring to their supervisors name in the message
- Another tactic is to split phishing email into groups such as by departments, or to tie phishing emails into topical or popular events
- Test them with the latest social engineering tactics and current event templates

Security Awareness Training Program That Works

- Drawn from a data set of **over six million users**
- Across **nearly 11K organizations**
- Segmented **by industry type** and **organization size**
- **241,762** Phishing Security Tests (PSTs)



Thank You!

Erich Kron – Security Awareness Advocate
ErichK@KnowBe4.com | @KB4Erich | @ErichKron

KnowBe4
Human error. Conquered.

Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com

BIG UNIVERSITY 2018

Owner / Principal Track

SESSION 3

Cyber Risk & Insurance: A 2018 Perspective on Claims & Coverage

McConkey Insurance & Benefits

Cyber

Every company has cyber threats

Disclaimer

The material in this presentation does not cover all possible cyber threats that may exist, does not identify potential controls for those risks, and does not constitute legal advice.

This material is not intended as advice to you or your insureds about specific risk control practices. Travelers disclaims all forms of warranties whatsoever, without limitation and implementation of any risk control practices suggested by this presentation is at your insured's sole discretion.

The material in this presentation does not amend, or otherwise affect, the provisions or coverages of any insurance policy issued by Travelers.

This presentation is not a representation that coverage does or does not exist for any particular claim or loss under any insurance policy.

Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy provisions, and any applicable law.

Availability of coverages referenced in this presentation may depend on state regulations.

Also note:

This presentation material is about coverages generally available in the marketplace, and is not based specifically on Travelers products.

In the news


PRIVACY BREACHES BOOST NEED FOR CYBER INSURANCE COVERAGES
The company reached a settlement with the Federal Trade Commission in early 2013. The company must
CYBER LIABILITY IS A NEW FRONTIER BOTH FOR INSURERS AND THE LEGAL SYSTEM
New Cyber Threats and Ways to Meet Them
Major companies keeping cyber attacks secret from SEC and investors
GROWING RISKS, MUDDY LEGAL WATERS POINT TO NEED FOR CYBER LIABILITY COVERAGE

The regulatory environment

State Data Breach Laws

Children's Online Privacy Protection Act **(COPPA)**

Health Insurance Portability & Accountability Act **(HIPAA)**

Federal Information Security Management Act **(FISMA)**

EU Data Protection Directive

Health Information Technology for Economic & Clinical Health Act **(HITECH Act)**

Gramm-Leach-Bliley

Securities and Exchange Commission **(SEC)**

FDIC and **FFIEC**

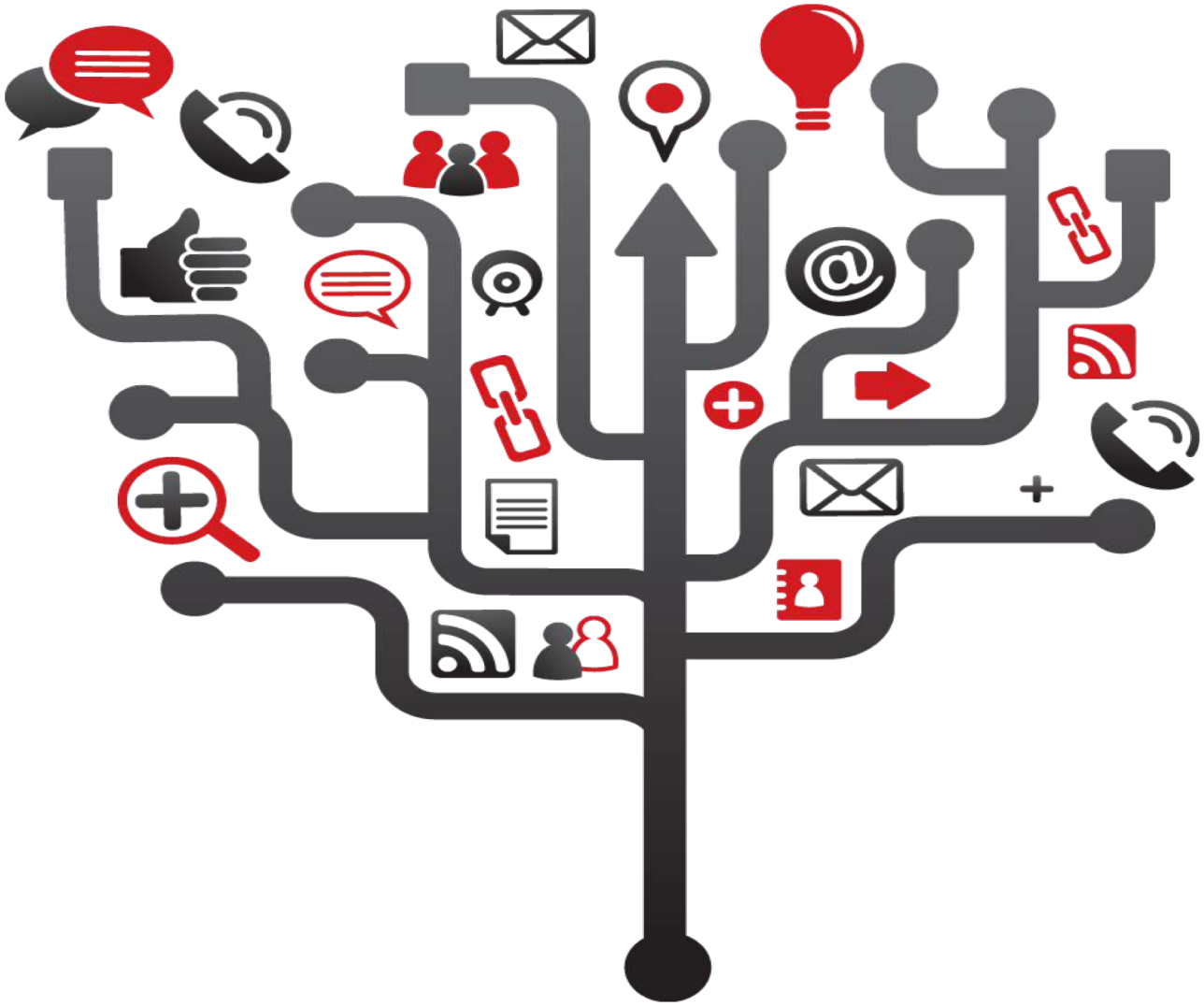
Sarbanes-Oxley

Payment Card Industry Data Security Standard **(PCI-DSS)**


Q
U
i
Z

Interconnectivity

Think of all the places
your personal information resides
and all the ways
it can be shared or transferred



How breaches can occur

E-mail: The #1 attack vector last year

Overall email malware rate		
2014	**2015**	**2016**
1 in 244	1 in 220	1 in 131

Email malware rate by company size	
Company size	Malware Rate (1 in)
1 - 250	127
251 – 500	95
501- 1,000	139
1,001 – 1,500	224
1,501 – 2,500	104
2,501+	170

Source: Symantec™ Internet Security Threat Report, Volume 22, April 2017

Magnitude of cyber threats

926,528 Average records lost in a data breach

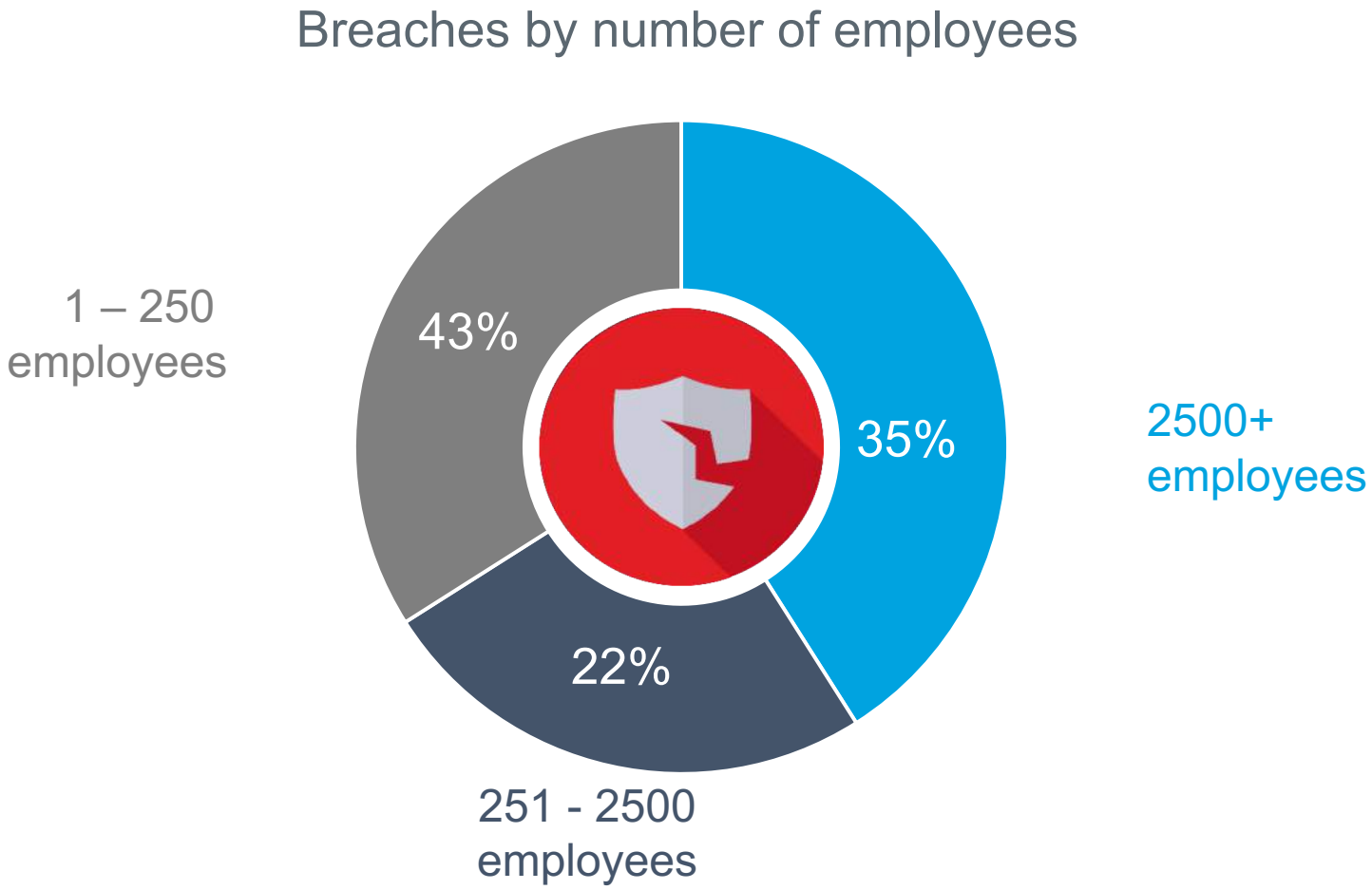
$5.3B Lost worldwide as a result of business email compromise fraud

85% Of surveyed executives reported experiencing cyber attach or breach

Sources: Symantec™, Internet Security Threat Report, Apr. 2017; Federal Bureau of Investigation, Public Service Announcement I-050417-PSA, May 2017; Kroll, Global Fraud & Risk Report, Jan. 2018

“Only large organizations are targets.”

Small and mid-sized firms are just as exposed to data breaches as large firms



Source: Symantec™ Internet Security Threat Report 2016

ANY business can be a target

Not solely an IT issue

If you have employees, you have exposure:

- Malware and viruses due to internet or email activities
- Leaving paper records in public
- Misplaced or stolen mobile devices
- Inadvertent emails
- Phishing and spear phishing

Hacking: Vulnerabilities and exploits

357M new malware variants in 2016 alone

Malware is still on top in its many forms

- Trojans, ransomware, worms
- Java downloaders leverage VB and Powershell scripts
- Windows, Mac, mobile devices all reported vulnerable

Source: Symantec™, Internet Security Threat Report, Apr. 2017

Ransomware: A problem that keeps getting worse

Prevalence

- 1,271 detections daily
- 463,000 per year - 36% increase

Ransom cost

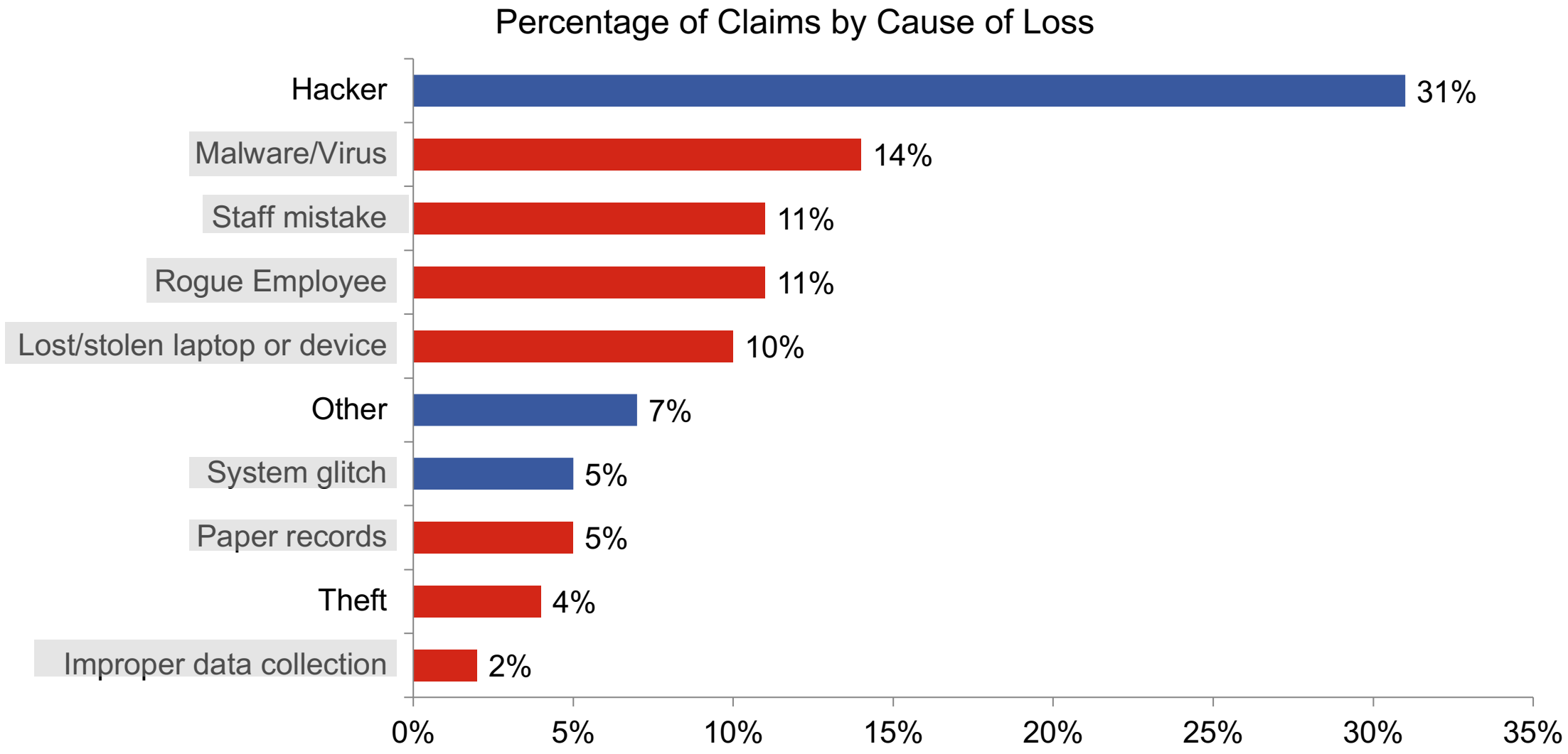
- 266% increase
- $1,077 per system up from $294

New ransomware families

- 101 new families
- 3x increase

Source: Symantec™ Internet Security Threat Report, Volume 22, April 2017

Employees can be involved in all the highlighted cause of loss



Source: NetDiligence® 2015 Cyber Claims Study

Costs of data breach

Information losses cost U.S. businesses an average of:

$221

per compromised record

$7.01M

total cost

Source: Ponemon Institute 2016 Cost of Data Breach Study, for surveyed companies that experienced a breach which required the company to notify victims under state law.

Why so expensive?

Security breach action steps

- Determining cause of security breach and persons whose identity information was accessed or acquired without their authorization
- Legal fees to determine applicable laws, develop materials and proactively defend firm from future liabilities
- Notify victims of breach, may include
  - Physical mailings
  - Emails
  - Call centers (incoming and outgoing)
- Potentially offering credit monitoring services

Summary: Potential impact of a cyber event

C O S T S

Costs of legal compliance

Forensics, legal consultants

Network damages and costs to repair or upgrade

Business interruption

Indemnify victims

Summary: Potential impact of a cyber event

…and more

C O S T S

Indemnify financial institutions

Defense costs

Injunctive relief

Damage to shareholders

Ticking time-bomb theory