Cybersecurity 101: For Non-IT Auditors

John B. Sapp Jr.

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

PROFESSIONAL DEVELOPMENT:

- **NATIONALLY-RECOGNIZED LEADER** IN AUDIT AND PEOPLE-CENTRIC© SKILLS TRAINING
- INSTITUTE OF INTERNAL AUDITORS ("IIA") REGISTRY OF CPE PROVIDERS (ONLY **6** FIRMS IN NORTH AMERICA!)
- OVER **170 FULL-DAY COURSES** ON AUDIT, IT AUDIT, ACCOUNTING, FINANCE, PERSONAL DEVELOPMENT AND PEOPLE-CENTRIC© SKILLS
- REGISTERED WITH **NASBA** TO OFFER CPE'S FOR ALL COURSES IN COURSE CATALOG (LIVE AND WEB-BASED)
- INTERACTIVE AND EDUCATIONAL COURSES FOR ALL LEVELS

EXECUTIVE RECRUITING:

- UNIQUE APPROACH TO FILLING POSITIONS, **INCLUDING PERSONALITY ASSESSMENT FOR CANDIDATE AND ORGANIZATION**
- EXPANSIVE NETWORK OF QUALIFIED CANDIDATES ACTIVELY LOOKING

STAFF AUGMENTATION:

- MARKET LEADER IN LOCATING COST-EFFECTIVE, RECOGNIZED RESOURCES IN ACCOUNTING, FINANCE, AUDIT AND IT
- ALL REQUESTS FILLED WITHIN **72 HOURS**

GOLDSRD SNAPSHOT

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

John B. Sapp Jr.

- **DIRECTOR, IT SECURITY & CONTROLS**
  - **ORTHOFIX MEDICAL INC.**
- **PUBLISHED AUTHOR (ARTICLES)**
  - CYBERSECURITY PEER REVIEW JOURNAL
  - PENTEST MAGAZINE
- **MEMBER**
  - FORBES TECHNOLOGY COUNCIL
  - CDM MEDIA ADVISORY BOARD
  - SECURE WORLD ADVISORY COUNCIL (SAN FRANCISCO CA, ATLANTA GA AND DALLAS TX)
- **FOUNDER**
  - CYBERSECURITY CONVERSATIONS – THE HYPE, HOPE AND HARSH REALITY

CERTIFICATIONS:

- HCISPP – SINCE 2013
- CRISC – SINCE 2011
- CGEIT - SINCE 2009
- CISSP - SINCE 2008

HONORS & AWARDS:

- 2013 INFORMATION SECURITY EXECUTIVE OF THE YEAR (CENTRAL)
- 2012 TBS CYBER SECURITY VISIONARY AWARD
- 2012 FINALIST – INFORMATION SECURITY EXECUTIVE OF THE YEAR (NORTH AMERICA)
- 2010 FINALIST – INFORMATION SECURITY PROJECT OF THE YEAR (NORTH AMERICA)
- 2010 FINALIST – INFORMATION SECURITY EXECUTIVE OF THE YEAR (WEST)

John B. Sapp, Jr.

- INDUSTRY RECOGNIZED THOUGHT LEADER AND CYBER VISIONARY
  - Invited Guest to The White House Colloquium for National Strategy for Trusted Identities in Cyberspace (NSTIC)
  - Cybersecurity Peer Review Journal (Inaugural Edition)
  - MISTI Security Leadership Exchange
  - Named 2012 TBS Cybersecurity Visionary

OBJECTIVES

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Cybersecurity 101: Objectives

- Cybersecurity Background and Overview
- Cybersecurity Trends & Insights
- Understand Cybersecurity Terminology
- Understand Key Controls for Cybersecurity Risk Management
- Understand Cybersecurity Frameworks
- Understand the Approach to Cybersecurity Risk Audit and Assessment

Group Discussion:
What Do You Want To Learn Today?

Time Allotted: 15 Minutes

GOLD SRD

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Cybersecurity Background

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

What is Cybersecurity?

Cybersecurity refers to the technologies, processes, and practices designed to protect an organization's information assets — computers, networks, programs, and data — from impact related to unauthorized access, unauthorized alteration and availability.

- Confidentiality
- Integrity
- Availability


Understanding Cybersecurity
Cybersecurity involves "threat actors" that want to obtain unauthorized access to your data and systems, and how individuals and companies can defend against these attacks. It is our goal to educate people of all disciplines about Cybersecurity and how we can all make a difference.

Cybersecurity Background

- **Who Are The Threat Actors?**
  - Threat actors come in many different forms, some obvious and some not so obvious:
    - Insider (employees, vendors, other trusted individuals)
    - Hackers
    - Cyber-criminals
    - Foreign governments and Intelligence agencies
    - Terrorists
    - Organized crime
    - Hactivists (i.e. Anonymous)

Cybersecurity Background

- **What Are The Threat Actors Seeking?**
  - Threat actors want data and secrets, and/or to blackmail/extort money from your organization
    - Usernames and passwords
    - Sensitive company documents
    - Protected Health Information (PHI)
    - Credit card and banking information
    - Export controlled technologies
    - Intellectual property and sensitive technological documents
    - Personal Identifying Information (PII)
    - Contact lists (emails, phone directories, etc.)
    - Confidential Emails

Group Discussion:
Calculating The Cost of A Breach

Time Allotted: 15 Minutes

State of Cybersecurity 2019

- https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019

What is the Cost of a Breach?

- 2018 Cost of a Data Breach Study
  - Independently conducted by Ponemon Institute and released July 2018
  - Benchmark research sponsored by IBM Security
  - Conducted interviews with more than 2,200 IT, data protection, and compliance professionals from 477 companies that have experienced a data breach over the past 12 months.

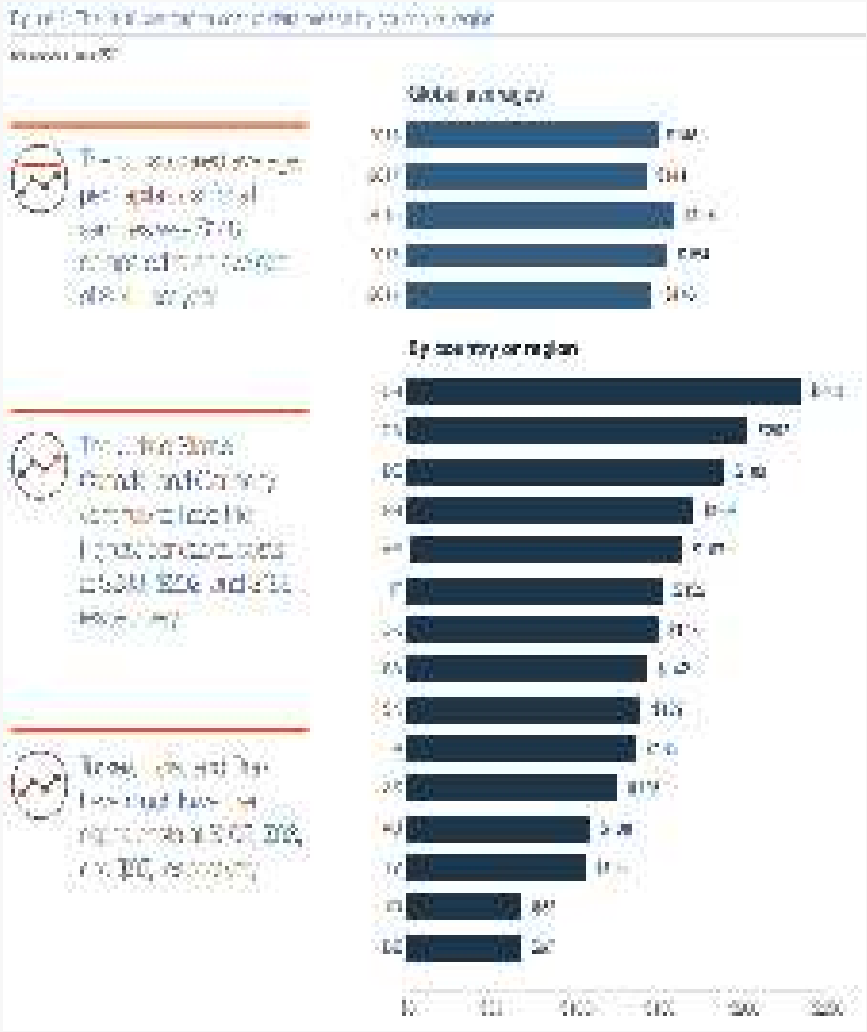
- Average total cost of a data breach: **$3.86M**
  - Increased 6.4% from 2017 ($3.62M)
- Average cost per lost or stolen record: **$148**
  - Increased 4.8% from 2017 ($141 per record)

Global Study at a Glance

- Average size of a data breach increased by **2.2%**
- Likelihood of a recurring material breach over the next two years: **27.9%**
- Average cost savings with an Incident Response team: **$14 per record**

SOURCES: Ponemon International Data Breach Statistics

Global Study at a Glance



SOURCES: Ponemon International Data Breach Statistics

Global Study at a Glance

- First time influence of **security automation** and **IoT devices** researched
  - Average cost of a breach for organizations that deploy security automation is **$2.88M**
  - Without automation, estimated cost is **$4.43M**
  - Extensive use of IoT devices increases cost $5 per compromised record

Main Root Causes

- Malicious or criminal attacks are the cause for most data breaches

Figure 8. Distribution of the benchmark sample by root cause of the data breach

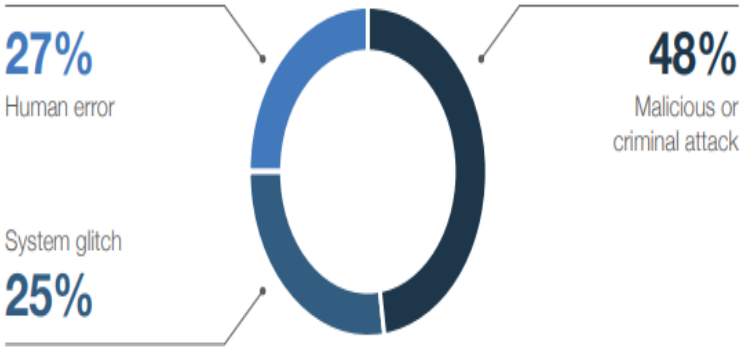
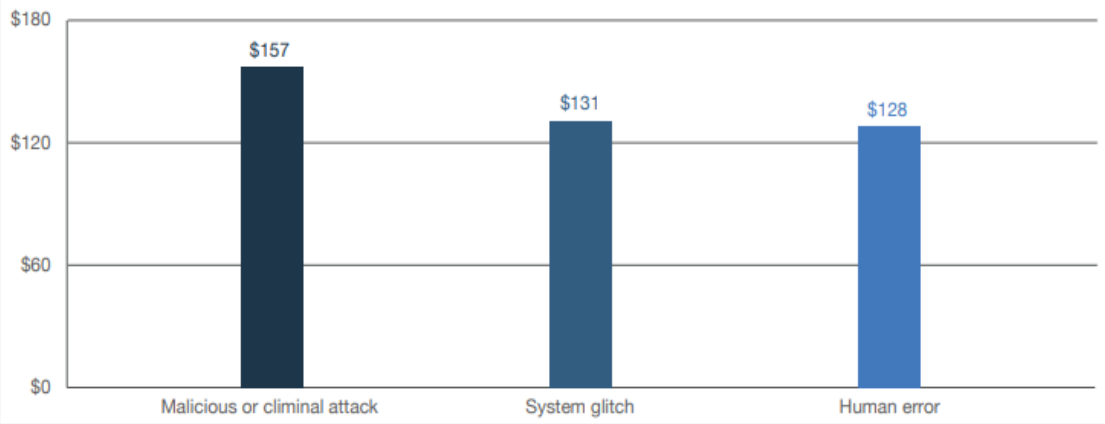


Figure 9. Per capita cost for three root causes of the data breach

Measured in US$

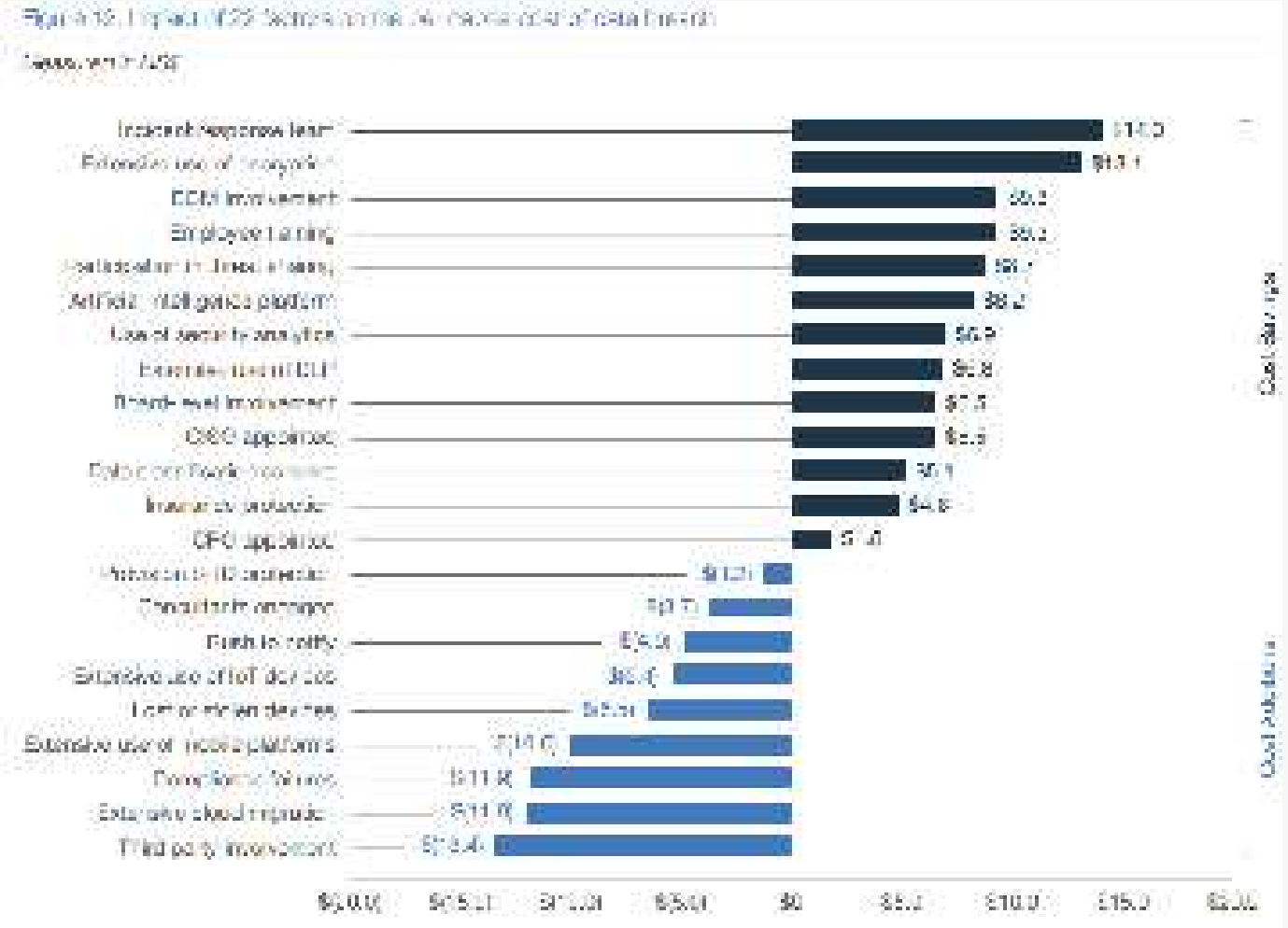


- Malicious or criminal attacks are the costliest

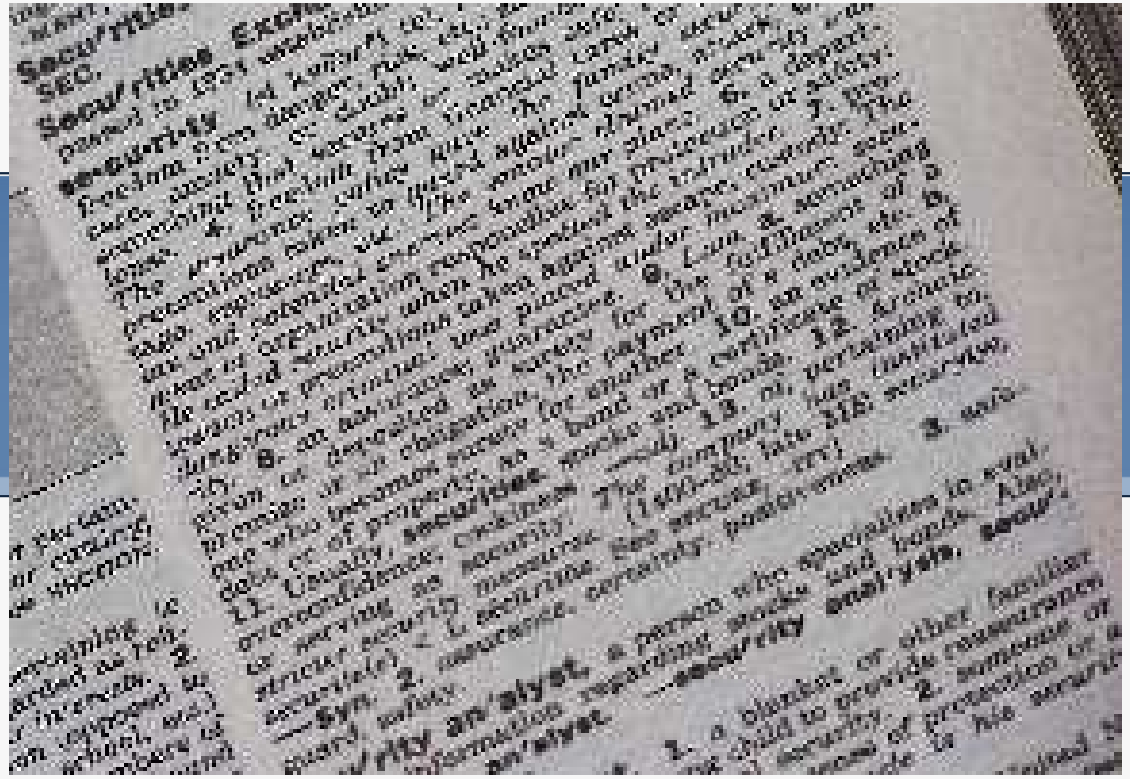
SOURCES: Ponemon International Data Breach Statistics

Factors that Influence Cost of a Breach

- Certain factors decrease or increase the cost of a data breach



SOURCES: Ponemon International Data Breach Statistics



CYBERSECURITY TERMINOLOGY

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Cybersecurity Terminology

- **Intrusion Detection**
  - The process and methods for analyzing information from networks and information systems to determine if a security breach or security violation has occurred.
- **Exploit**
  - A malicious application or script that can be used to take advantage of a computer's vulnerability.
- **Malware**
  - An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include: viruses, trojans, worms and ransomware.
- **Breach**
  - Any incident that results in unauthorized access of **data**, applications, services, networks and/or devices by bypassing their underlying **security** controls

Cybersecurity Terminology

- **Ransomware**
  - A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered.
- **Bot / Botnet**
  - A type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer.
- **Distributed Denial of Service (DDoS)**
  - A form of cyber attack. This attack aims to make a service such as a website unusable by "flooding" it with malicious traffic or data from multiple sources (often botnets).
- **Phishing / Spear Phishing**
  - A technique used by hackers to obtain sensitive information. For example, using hand-crafted email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.

Overview of A Cyber Attack

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

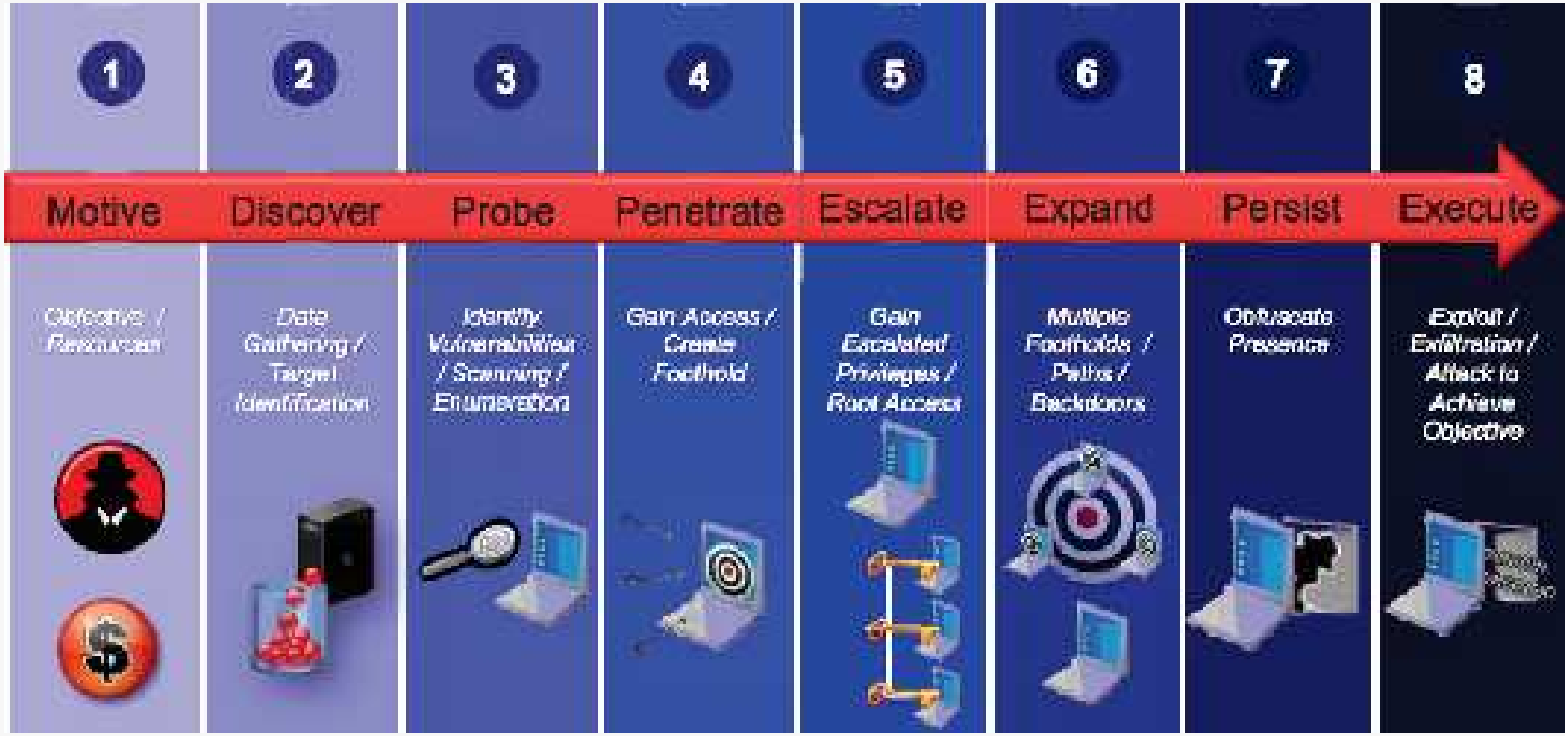
Cyber Attack Overview

- It's not IF but WHEN a cyber attack will occur against your organization
- Cyber attacks target organizations of ALL size (even individuals)
- Every organization has information that is meaningful to a cyber attacker

Cyber Attack Overview

- **What Activities Does A Cyber Attacker Use?**
  - Reconnaissance
  - Intrusion / Delivery
  - Exploitation / Obtaining Credentials
  - Pivoting / Lateral Movement
  - Installation
  - Data Exfiltration / Manipulation
  - Maintaining Persistence

Cyber Attacker Activities



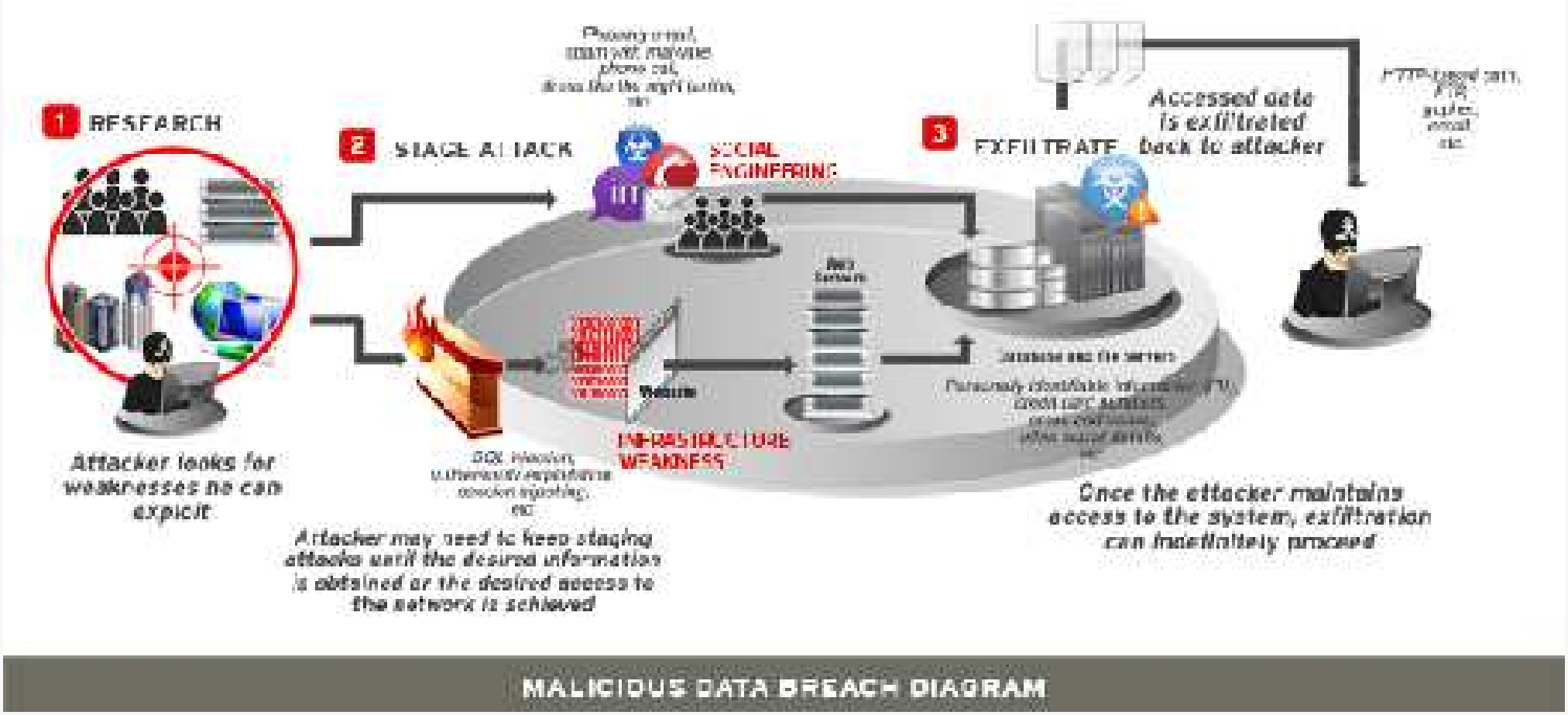
Cyber Attack Overview

- **Who is Responsible for Protecting against Cyber Attacks? EVERYONE!**
  - Some signs to look for and report include:
    - System failure or disruption
    - Suspicious or over-zealous questioning
    - Unauthorized access to systems and facilities
    - Unauthorized or unexpected changes
    - Suspicious emails
    - Unauthorized use
    - Strange system behavior

Cybersecurity Background

- **How do Threat Actors Compromise Systems?**
  - There are many methods that threat actors use to gain unauthorized access to systems
    - Malware (malicious software) / Viruses
    - Social Engineering
    - Phishing or Spear Phishing
    - Unpatched, outdated or vulnerable systems and software
    - Weak or default passwords
    - Stolen credentials
    - Technical methods (SQL injection, cross-site scripting, etc.)

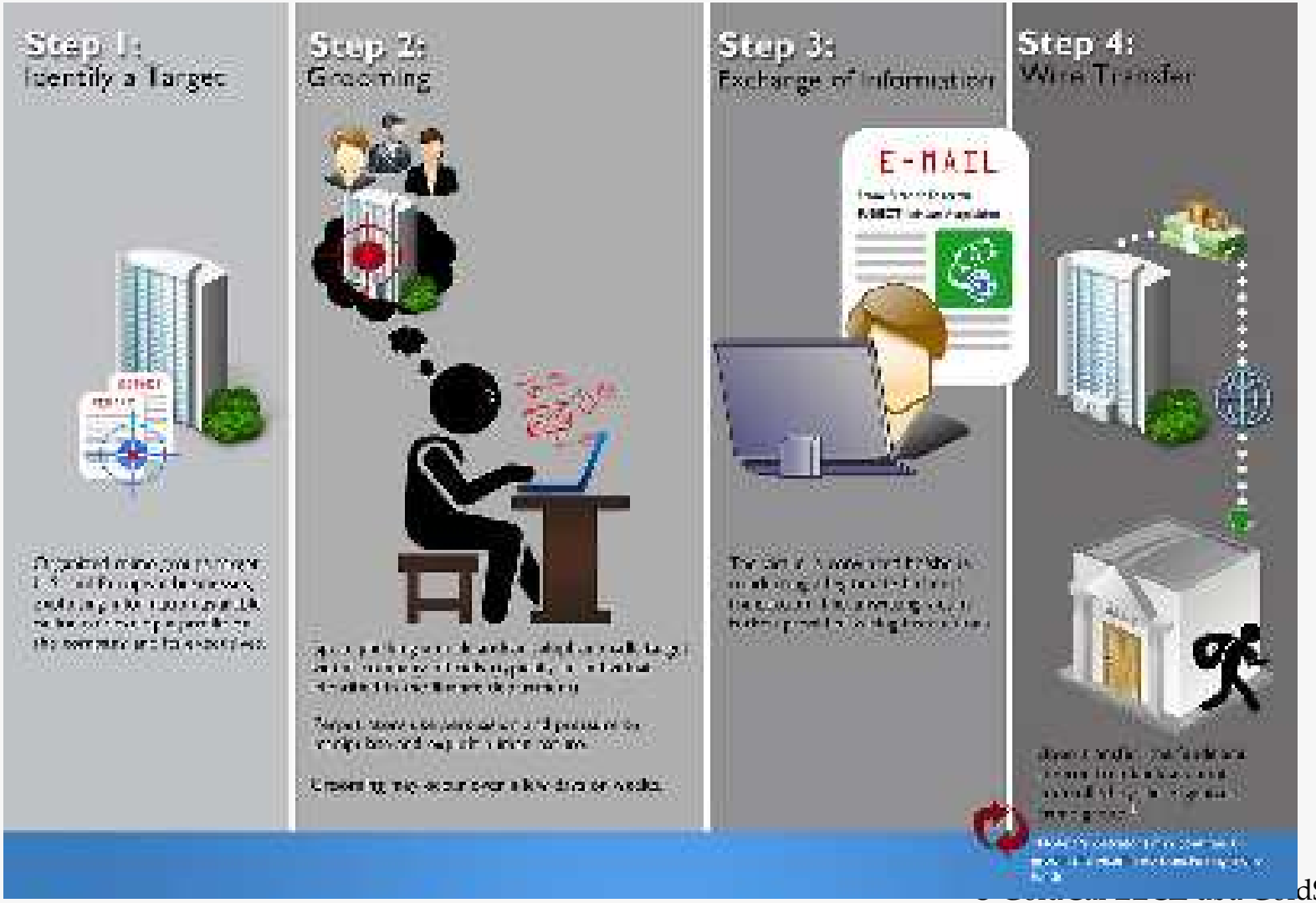
Anatomy of a Data Breach



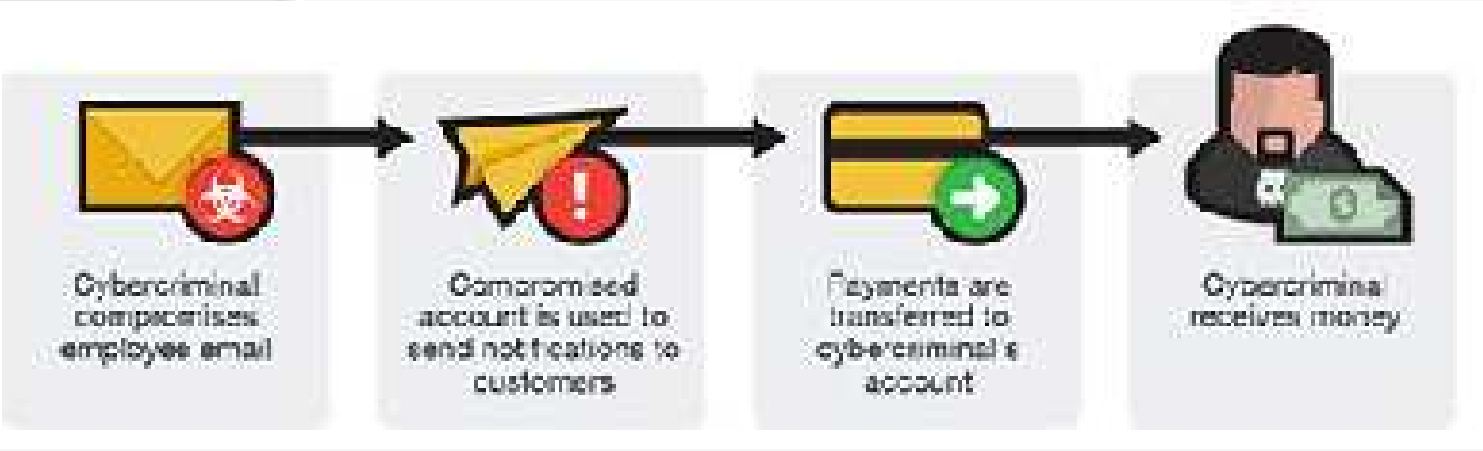
MALICIOUS DATA BREACH DIAGRAM

SOURCE: Trend Micro Threat Encyclopedia

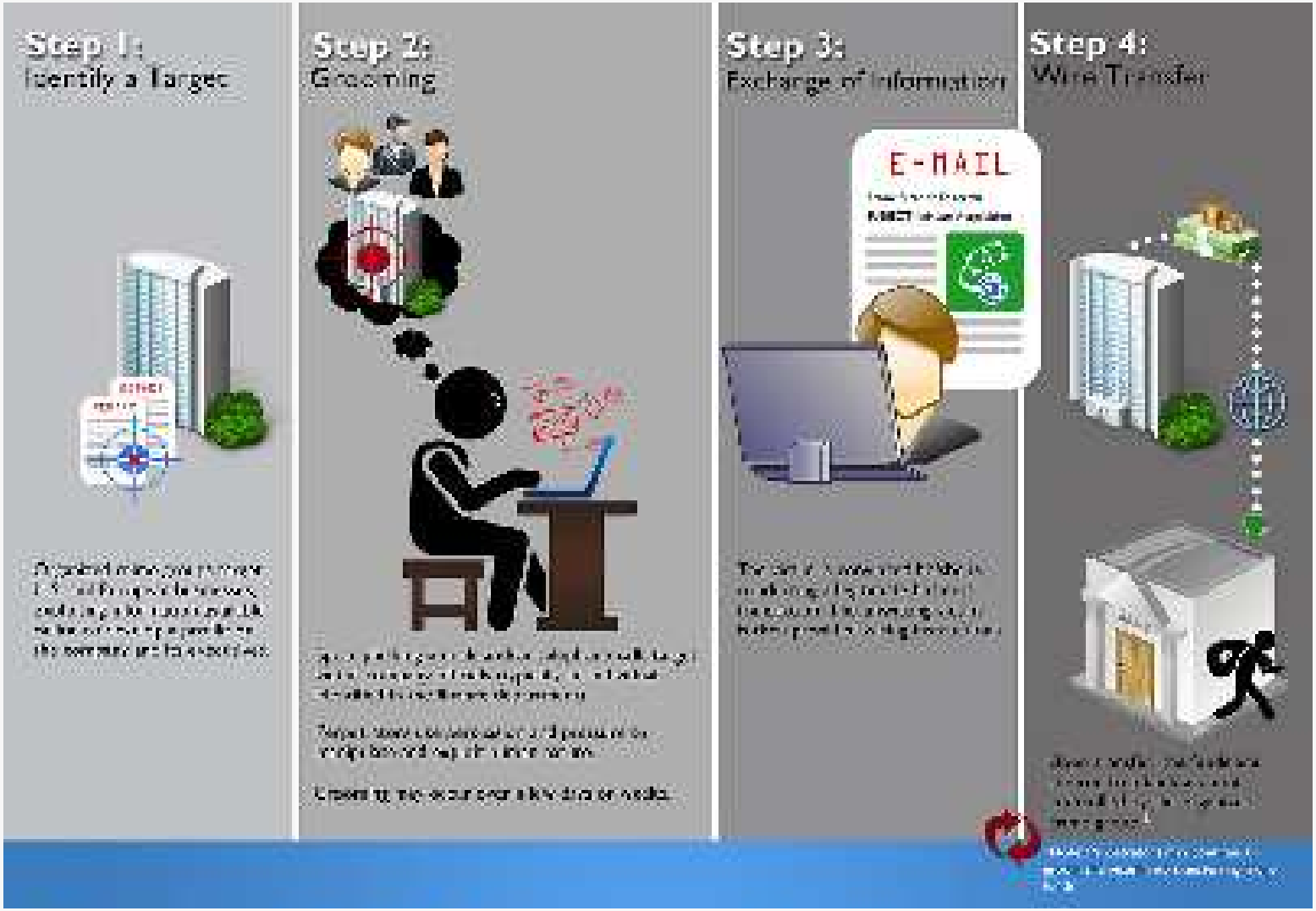
Anatomy of a Data Breach



BUSINESS EMAIL COMPROMISE



THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT



BEC - Overview

- Target employees with access to company finances and trick them into making wire transfers to bank accounts thought to belong to trusted partners—except the money ends up in accounts controlled by the criminals
- Techniques include:
  - Spear-phishing
  - Social engineering
  - Identity theft
  - E-mail spoofing
  - Malware
- According to the FBI's Internet Crime Complaint Center (IC3), "the BEC scam continues to grow, evolve, and target businesses of all sizes. Since January 2015, there has been a 1,300 percent increase in identified exposed losses, now totaling over $3 billion"

SKIMMING

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

ATM & Gas Pump Skimming

- Similar to identity theft for debit cards: Thieves use hidden electronics to steal the personal information stored on your card and record your PIN number to access all that hard-earned cash in your account
- Card reader placed over the ATM's or gas pump real card slot
- When you slide your card into the ATM, you're unwittingly sliding it through the counterfeit reader, which scans and stores all the information on the magnetic strip

ATM & Gas Pump Skimming - Stats

- During the first six months of 2017, the number of compromised ATMs and point-of-sale devices jumped 21 percent, compared to the first six months of 2016, according to FICO
- 30% increase in compromised devices from 2015 to 2016 & 70% increase in compromised cards during that time, according to FICO
- Large increase in gas pump skimmers
  - Florida, for example, tracks the number of skimmers found at gas stations. Through July 18, 2017, authorities had found 315 skimmers, nearly triple the number found in the same period in 2016

How big is the risk of gas pump skimming? According to the National Association for Convenience Stores:

- 37 million Americans refuel every day
- Of them, 29 million pay for fuel with a credit or debit card
- When skimming occurs at a gas station, it usually takes place at only one pump
- Single compromised pump can capture data from 30 to 100 cards per day

AUTHENTICATION & SYNTHETIC ID'S

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Synthetic ID's

- Take personal information from various individuals and combining them into a new, hybrid identity that only exists in the virtual world
- Use this information to open new bank or credit card accounts
- Financial institutions usually are the victims of the fraud because there's no individual victim; losses generally get written off as bad debt

MOBILE BANKING

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Mobile Banking Risks

- Smart phone attacks will target the information on the device, as well as the information the device can access and the messages it receives
- New payments systems using smart phones will be hit with malware attacks on the devices and the apps they are running
- Paypal, Venmo, Velle

Zelle Scam

- Defrauding consumers who believe the service includes the same protections they've come to expect from PayPal
- Scam:
- Seller will ask the buyer to pay them through Zelle instead of PayPal
- Seller will keep the money, then shut down their bank account, and disappear
- Tickets, or whatever else they were purportedly selling, never arrive
- In other cases, the scammer may not even need to go to that extreme because the victim's bank just tells their customer there's nothing they can do, since the customer had authorized the Zelle transaction

Real World, Recent Examples

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Data Breaches

- **Reported 139,731,894 million records leaked**
  1. Confluence Health discloses patient data breach after employee email account hacked
  2. LifeLock Bug Exposed Millions of Customer Email Addresses
  3. Patient data found in Helsinki street
  4. Patients' health records stolen from gas station
  5. Hackers Breach Russian Bank and Steal $1 Million Due to Outdated Router
  6. Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

Confluence Health

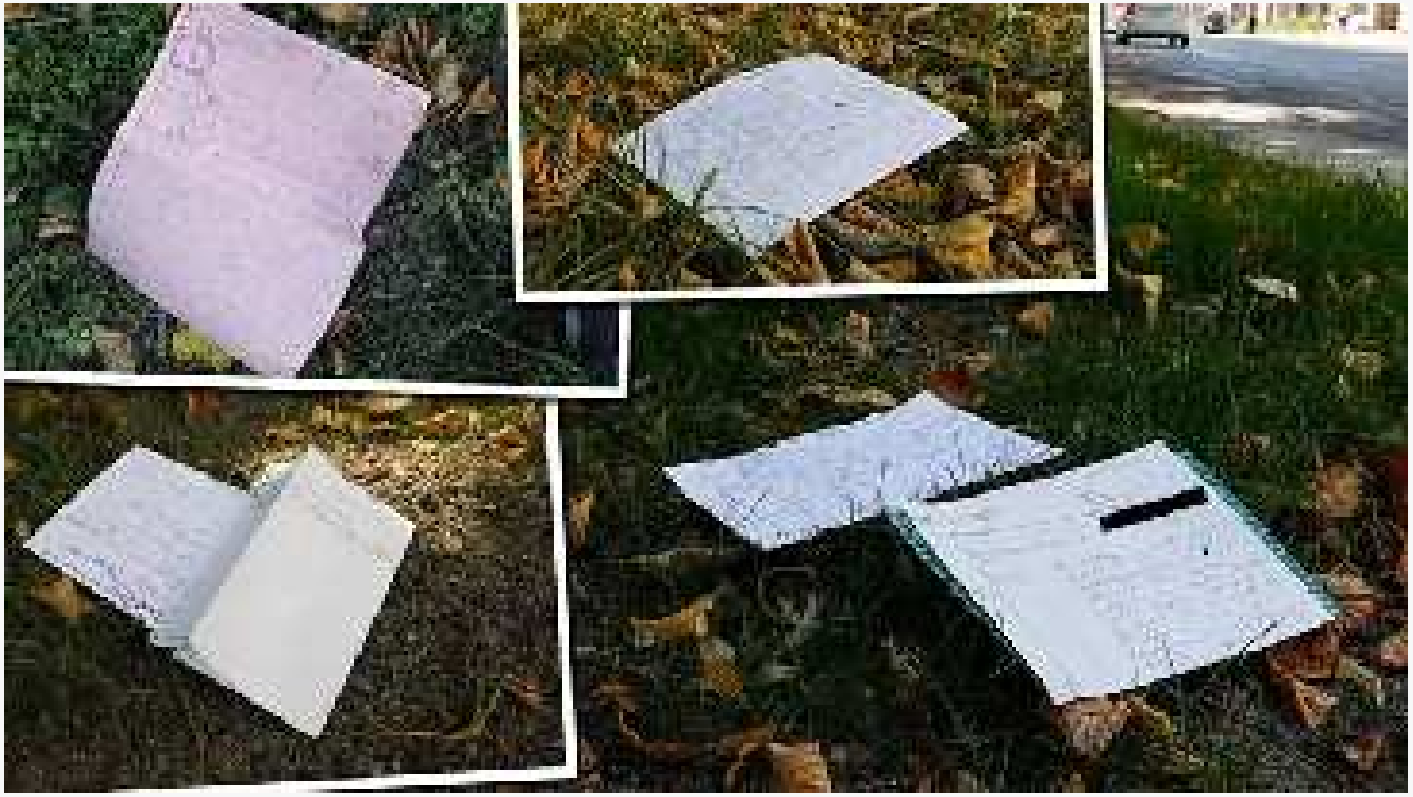
- Control Failure: Administrative (User), Technical (Access)
- Compromised credentials
- Unauthorized access
- Confidentiality breach

LifeLock

- Control Failure: Application (Secure SDLC, Fuzz testing)
- Simple script could have been used to exploit and harvest email addresses to use in a Phishing campaign

Helsinki Contraception Clinic

- Control Failure: Physical (Proper Disposal or Destruction)
- Confidentiality breach

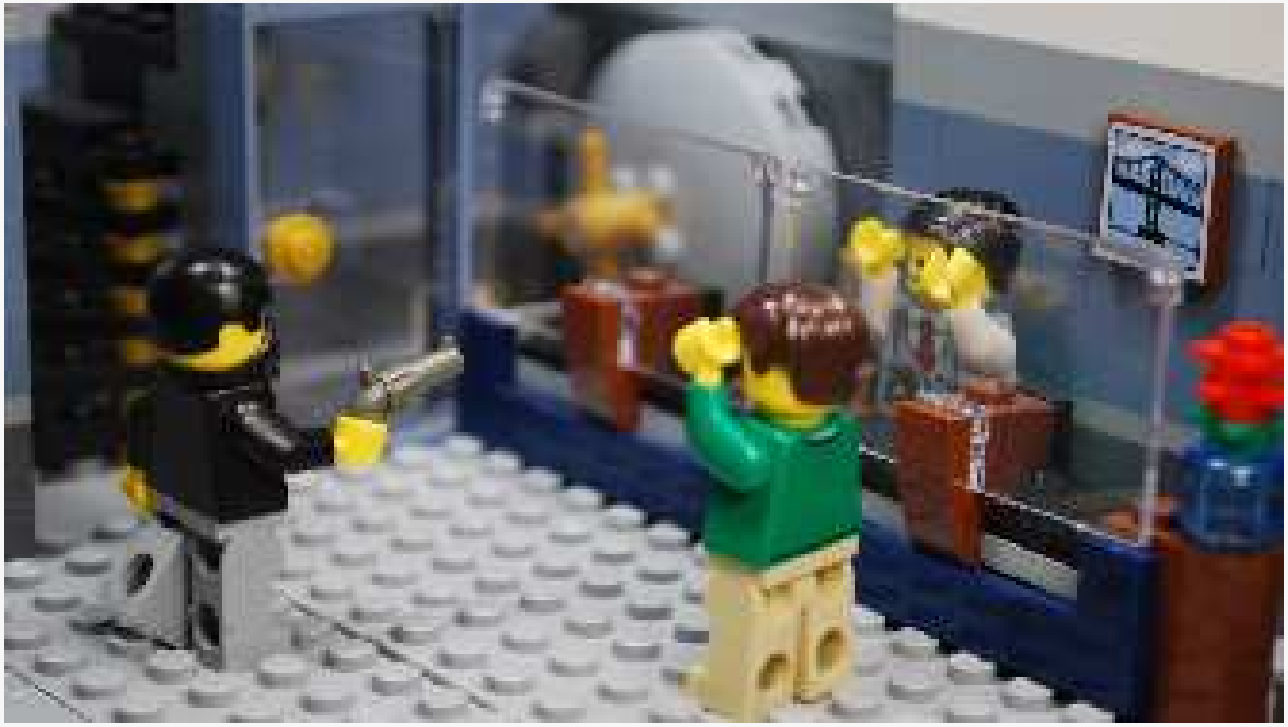


Roper Hospital

- Control Failure: Physical (Controlled access)
- Confidentiality breach
- Prior physical security control failure in May 2015

Russian PIR Bank

- Control Failure: Vulnerability Management (System Patching)
- Transferred approximately $1 million to 17 accounts at multiple Russian banks



Internet of Things (IoT) Attacks

- Casino high-roller data exfiltrated through IoT thermometer in a fish tank
- Baby monitors, automobiles, home security systems, etc.

Cyber Attacks and Ransomware

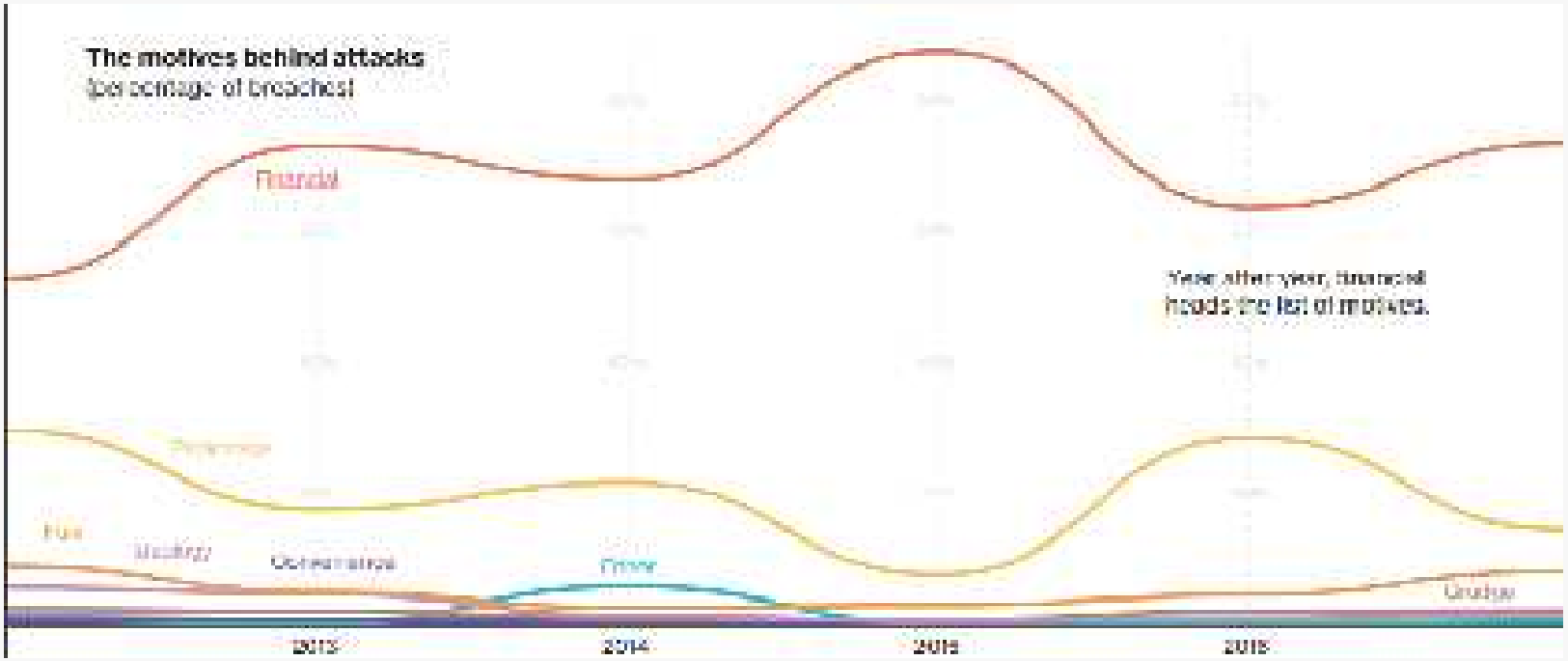
1. Mumbai: Ransomware hits Dadar CA's office, demands payment in bitcoins for decryption
2. Samsam infected thousands of LabCorp systems via brute force RDP
3. Long Beach Port terminal hit by ransomware attack
4. Another Crypto Fail: Hackers Steal $23.5 Million from Token Service Bancor

CYBERSECURITY INSIGHTS

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Data Breach Investigations Report (DBIR)

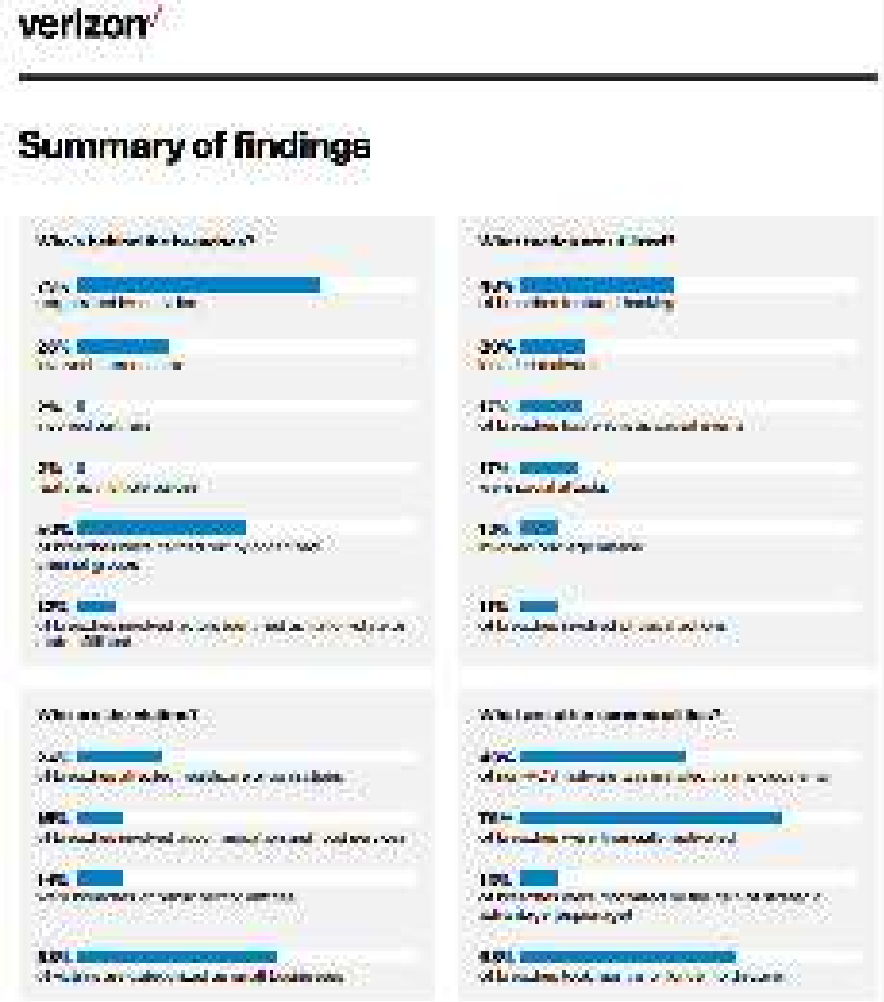
- By the numbers
  - 53,308 security incidents
  - 2,216 data breaches
- By the numbers
  - 65 countries
  - 67 contributors
  - 75% Financially motivated



SOURCE: 2018 Verizon Data Breach Investigation Report

Summary of Findings

- 73% Perpetrated by outsiders
- 48% Breaches featured hacking
- 49% Non-POS malware installed via malicious email
- 76% Breaches were financially motivated
- 68% Breaches took longer to discover
- 58% Victims categorized as small business



SOURCE: 2018 Verizon Data Breach Investigation Report

Social Attacks

- **Phishing and pretexting represent 98% of social incidents and 93% of breaches.**
- **Email continues to be the most common vector with 96%.**

Frequency	1,450 incidents, 381 with confirmed data disclosure
Top 3 patterns	Crimeware, Everything Else, and Cyber-Espionage represent 93% of all security incidents
Threat actors	99% External, 6% Internal, <1% Partner (breaches)
Actor motives	59% Financial, 38% Espionage (breaches)
Data compromised	47% Personal, 26% Secrets, 22% Internal, 17% Credentials

SOURCE: 2018 Verizon Data Breach Investigation Report

Top Targeted Industries & Data Types

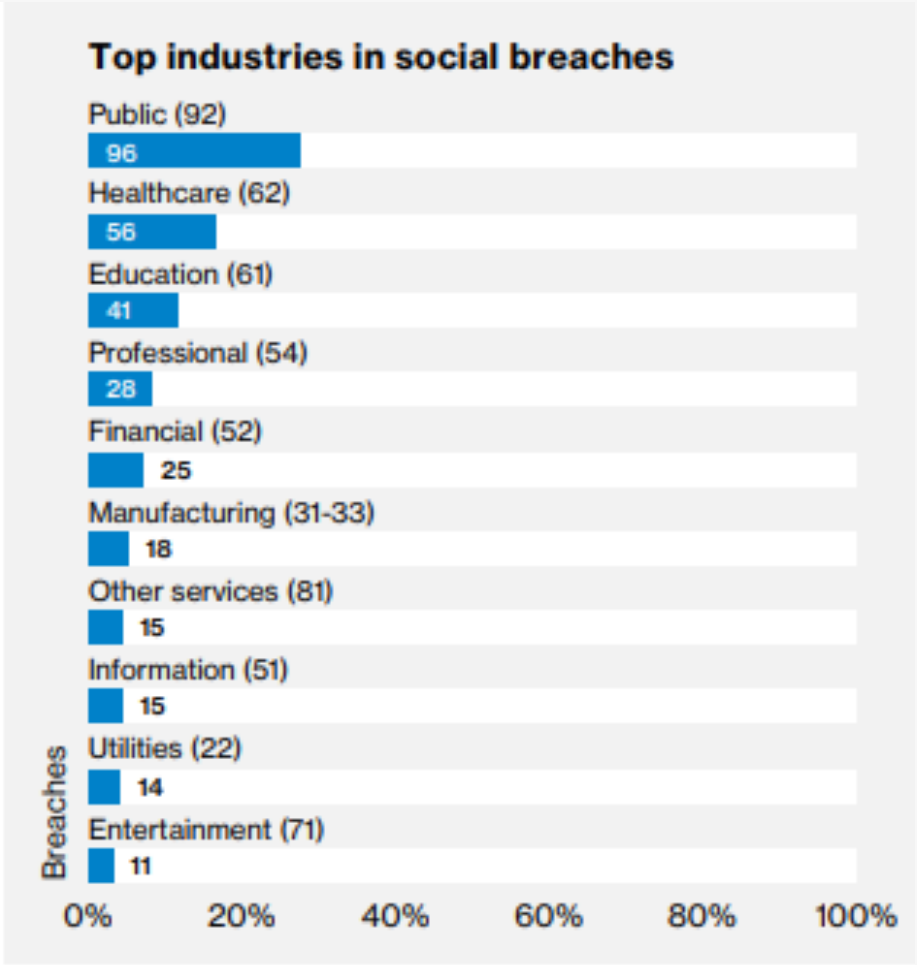


Figure 11. Top industries within Social breaches (n=351)

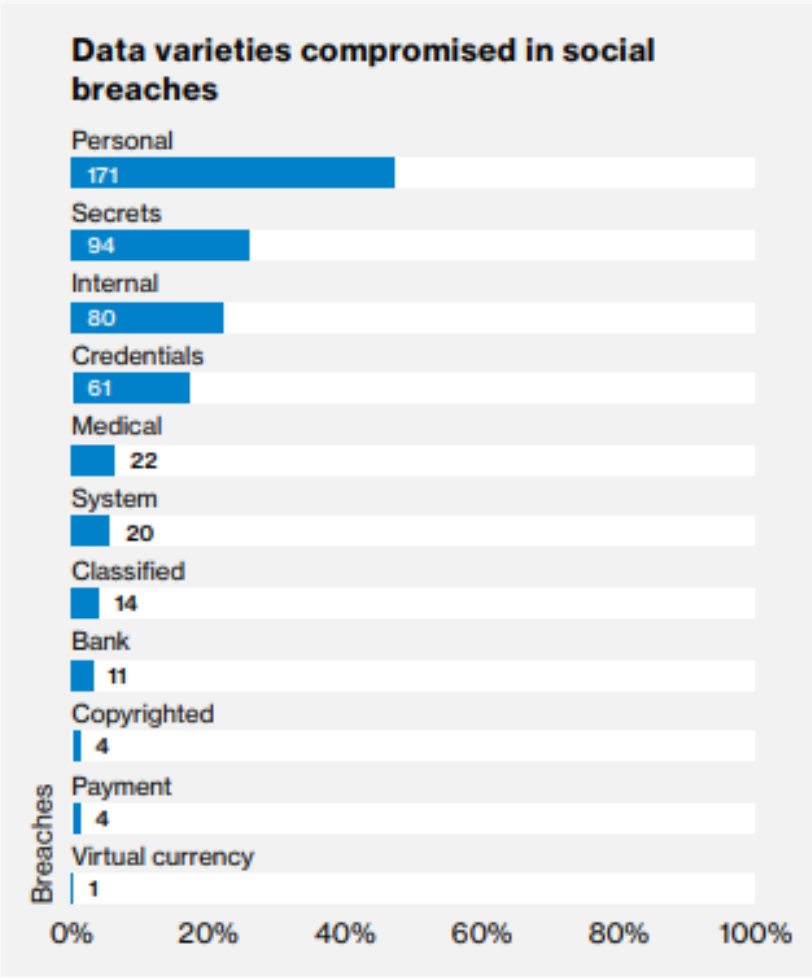


Figure 12. Data varieties compromised in Social breaches (n=362)

SOURCE: 2018 Verizon Data Breach Investigation Report

Top Attack and Asset Target

- Ransomware became an effective tool of choice in 2013
- User devices are the primary targets

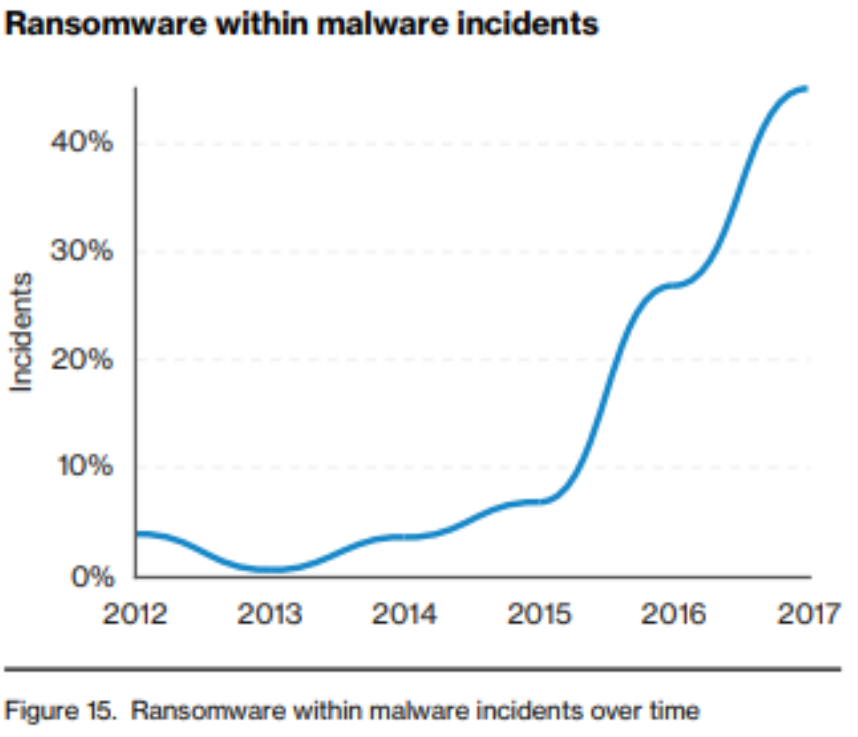
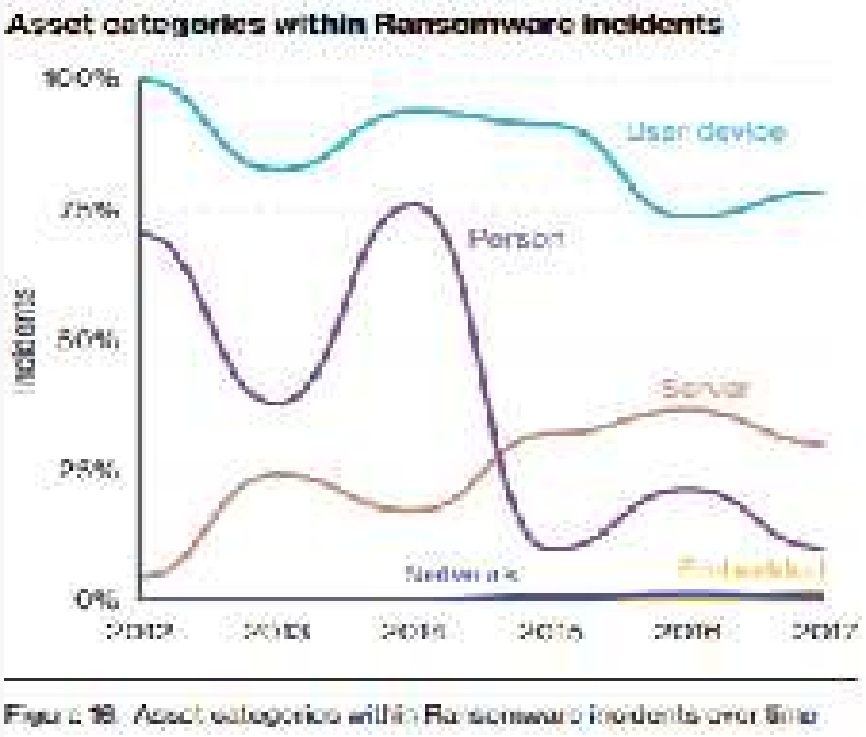
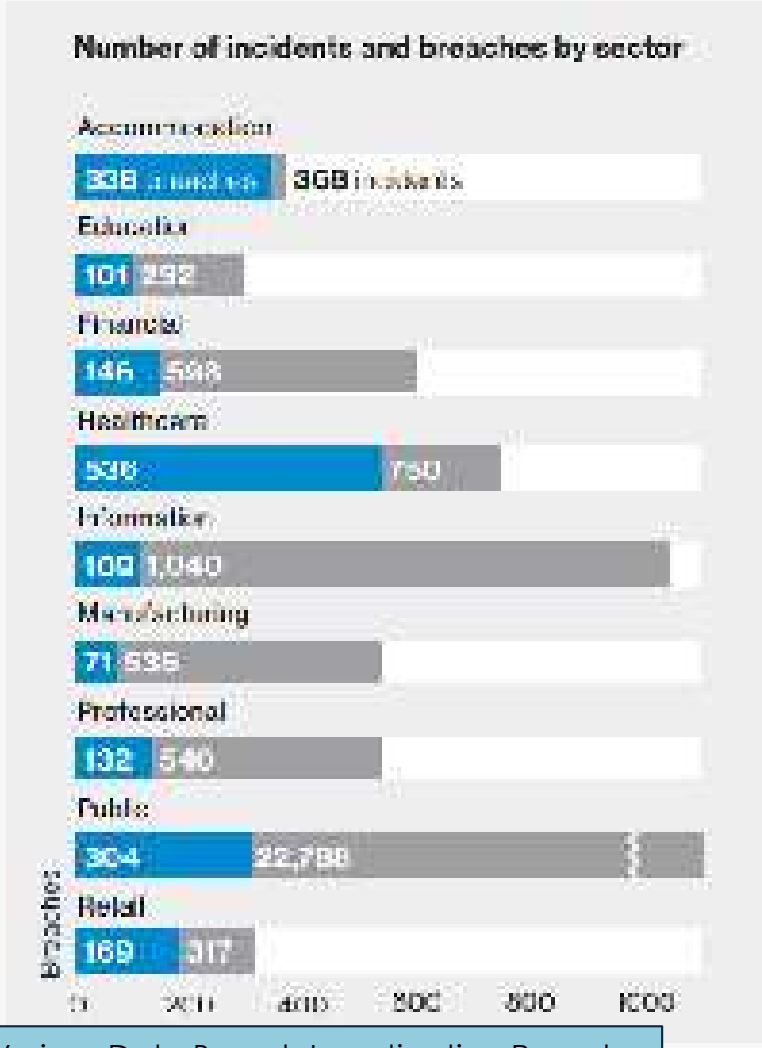


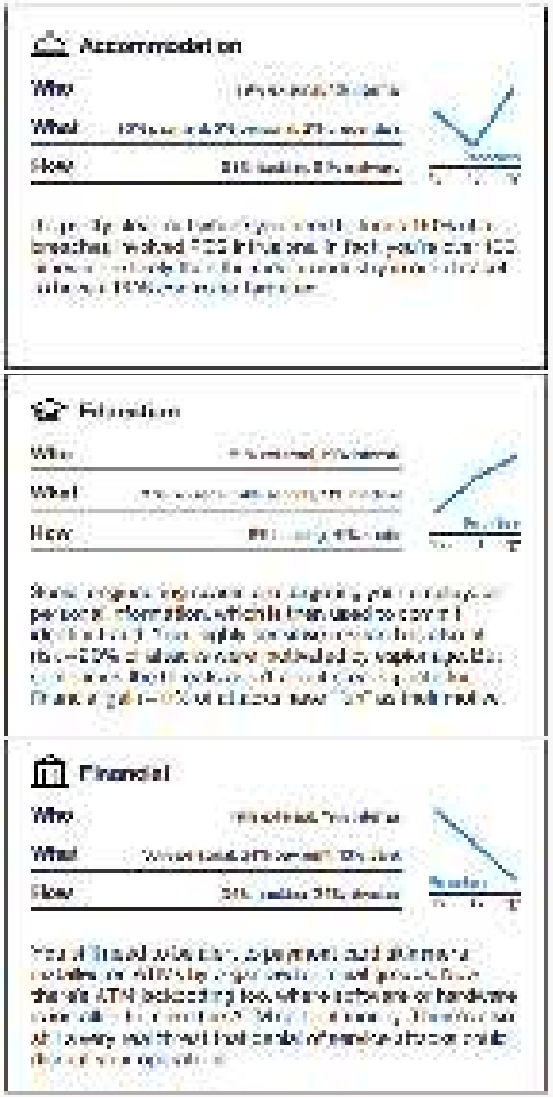
Figure 15. Ransomware within malware incidents over time



SOURCE: 2018 Verizon Data Breach Investigation Report

What's the Biggest Risk to Your Business?





SOURCE: 2018 Verizon Data Breach Investigation Report

Group Exercise: Targeted Attack Game

GOLD SRD

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Targeted Attack Game

- With all bad things in life, we like to believe that "it will never happen to us". Unfortunately the reality of targeted attacks against commercial organizations is such that many in the security world are characterizing it as a "when" rather than an "if".
- **You** will be put you in the driving seat. **You** are the **CIO** of a global organization called The Fugle, who is on the verge of making the first release of a biometrically authenticated mobile payment app.
- **You** will steer the project through its final stages, dealing with your internal security team, your colleagues in Marketing and PR and of course your CEO.

SOURCE: www.trendmicro.com

Targeted Attack Game: Characters

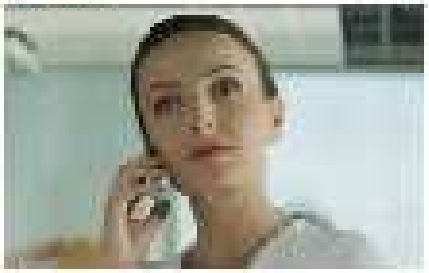
You

Vanessa

Randall

Julian

Melinda



Vic

Targeted Attack Game: Let's Play!

TREND MICRO

An educational game
brought to you by Trend Micro

TIME ALLOTTED: 30 MINUTES

CYBERSECURITY STRATEGY

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Cybersecurity Strategy Overview

- Identify a Cybersecurity Framework that best fits your organization
- Map organization's existing controls to the selected Cybersecurity Framework
- Assess and Manage the Risk
- Measure Progress and Maturity
- Continuously Monitor and Measure Security

GOLD NUGGET #1

- GTAG – Global Technology Audit Guide
- Prepared by The IIA, GTAG is written in straightforward business language to address timely issues related to information technology (IT) management, risk, control, and security
- **HERE'S THE KICKER** – IIA members access GTAG's **FREE**!

Cyber Strategy

Strategic Framework

- Select Baseline Framework
  - NIST Cybersecurity Framework
  - CIS Critical Security Controls
  - ISO 27001 Information Security Management System (ISMS)

CYBERSECURITY CONTROL FRAMEWORKS

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Why Use a Cybersecurity Framework?

- Using a known framework allows other stakeholders (your customers, commercial insurer, Board members, etc.) to have confidence that you are covering all areas and if you have a third-party attestation that you are meeting the requirements it is often accepted in lieu of having to complete lengthy questionnaires to confirm your controls and practices.

NIST CSF

- **National Institute of Standards and Technology Cybersecurity Framework**
  - https://www.nist.gov/cyberframework
  - This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

NIST CSF – Functions and Categories

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

CIS Critical Security Controls

- **Center for Internet Security**
  - **https://www.cisecurity.org/controls**
  - **Formerly SANS Top 20 Critical Security Controls**
  - The CIS Controls™ are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others.

CIS Critical Security Controls

CIS Controls™ V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

ISO 27000 Series

- **International Standards Organization**
  - http://www.iso27001security.com/html/27001.html
  - **ISO**/IEC **27001** is an information security standard, part of the **ISO**/IEC **27000** family of standards, of which the last version was published in 2013, with a few minor updates since then.
  - **ISO/IEC 27001 does *not* formally mandate specific information security controls** since the controls that are required vary markedly across the wide range of organizations adopting the standard.

GOLD NUGGET #2

- The use of a Cybersecurity Framework provides the foundation for a cybersecurity program
- The selection of a Cybersecurity Framework is a critical success factor and basis for a cybersecurity audit

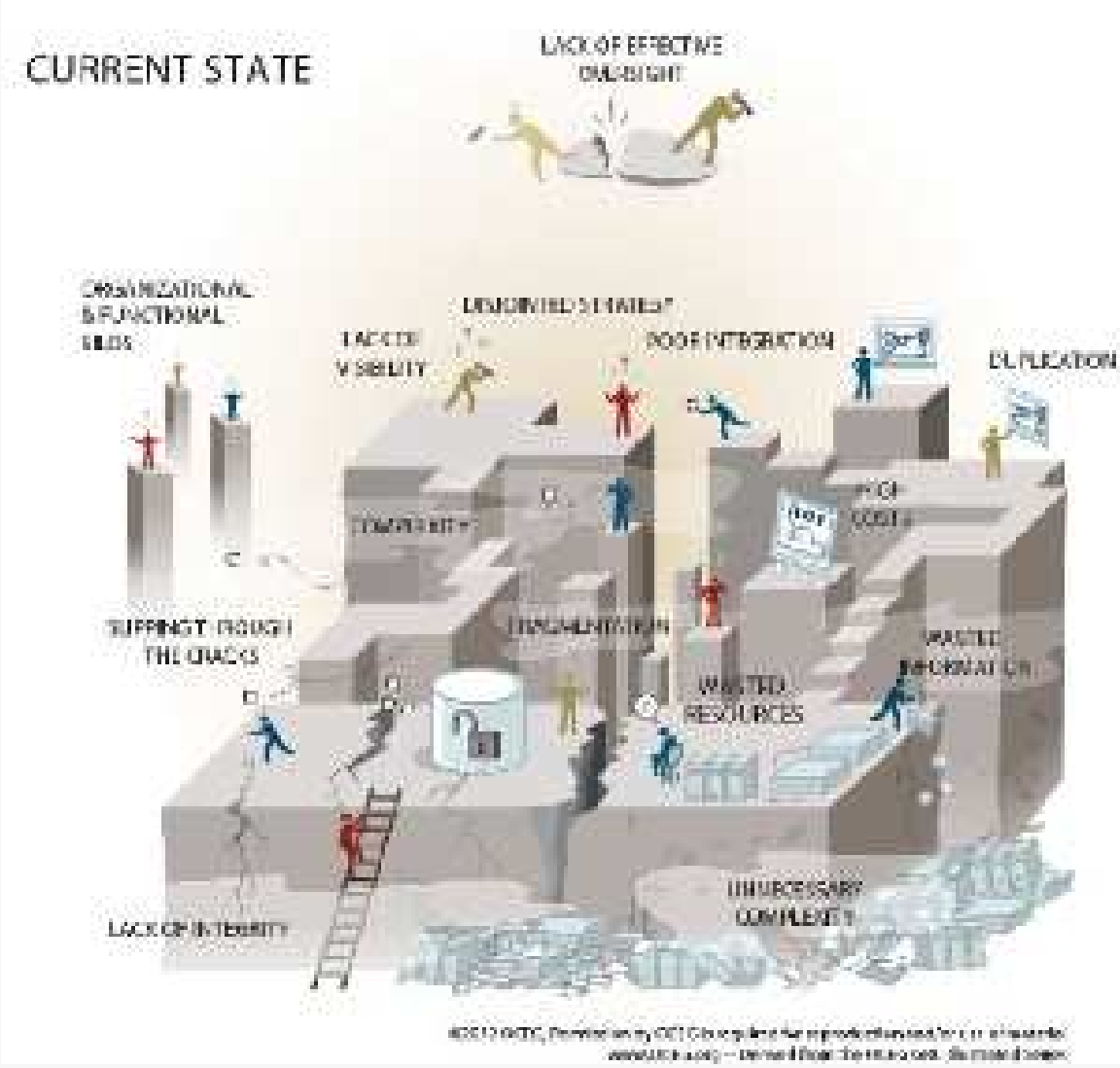
Cyber Strategy

Current State Analysis

- Measure current maturity
- Assess impact of current initiatives
- Identify key risks and challenges

Current State

- **The Problem**
  - Disjointed Strategy
  - Lack of Visibility
  - Fragmentation
  - Lack of Effective Oversight



THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Risk Assessment Results

Technical Vulnerabilities

- System Configurations
  - Excessive Privileges to Network File Shares
  - Weak or Default Passwords for Applications, Service Accounts, Operating Systems, Devices, Databases and End User Accounts
- Endpoint Security
  - Administrative Privileges
  - Mobile Device Management
- Network Security
  - Intrusion Detection and Intrusion Prevention
  - Network Access Control

Administrative Vulnerabilities

- Patch Management Process
- IT Policies and Standards
- Third-party Services Agreements
- Cloud Application Authorization
- Cybersecurity Incident Response
- Risk Mitigation, Risk Acceptance Process

Top 5 Cybersecurity Threats

- Cyber Extortion (Ransomware & Phishing)
- Internet of Things (IoT)
- Insiders (employees, vendors, partners)
- Distributed Denial of Service (DDoS)
- Mobile Devices

Top 5 Cybersecurity Risks

- Workforce and Third-party Service Providers
- Cloud Services and Cloud Applications (Shadow IT)
- Patch Management
- Incident Response Management
- Unsupported IT Systems and Applications

Cybersecurity Vulnerability Remediation

- Deployment of Next Generation Solutions
  - Advanced Secure Web Gateway
  - Advanced Endpoint Malware Protection
  - Advanced Email Threat Protection
  - Endpoint Protection (Encryption & Data Loss Prevention (DLP)
- Security Awareness Education & Training
- Global Security Operations Center (24x7x365)

Cybersecurity Risk Mitigation

- Development of IT Risk Management Plan
- Cybersecurity Insurance
- Information Security Program Maturity
- IT Policies and Standards
- Endpoint Management
- Mobile Device Management
- Cloud Access Security Management

Summary

Risk vs Threat vs Vulnerability

Risk is identified and managed through comprehensive evaluation and assessment of threats and vulnerabilities.

A + T + V = R

Asset + Threat + Vulnerability = Risk

Threat – Anyone or anything that can exploit a vulnerability (weakness), intentionally or accidentally and obtain, damage or destroy an asset.

"What we are trying to protect against."

Vulnerability – Weakness or gaps in a security program than can be exploited by threats to gain unauthorized access to an asset.

"Weakness or gap in our protection efforts."

Risk – The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

Risk is the intersection of assets, threats and vulnerabilities.

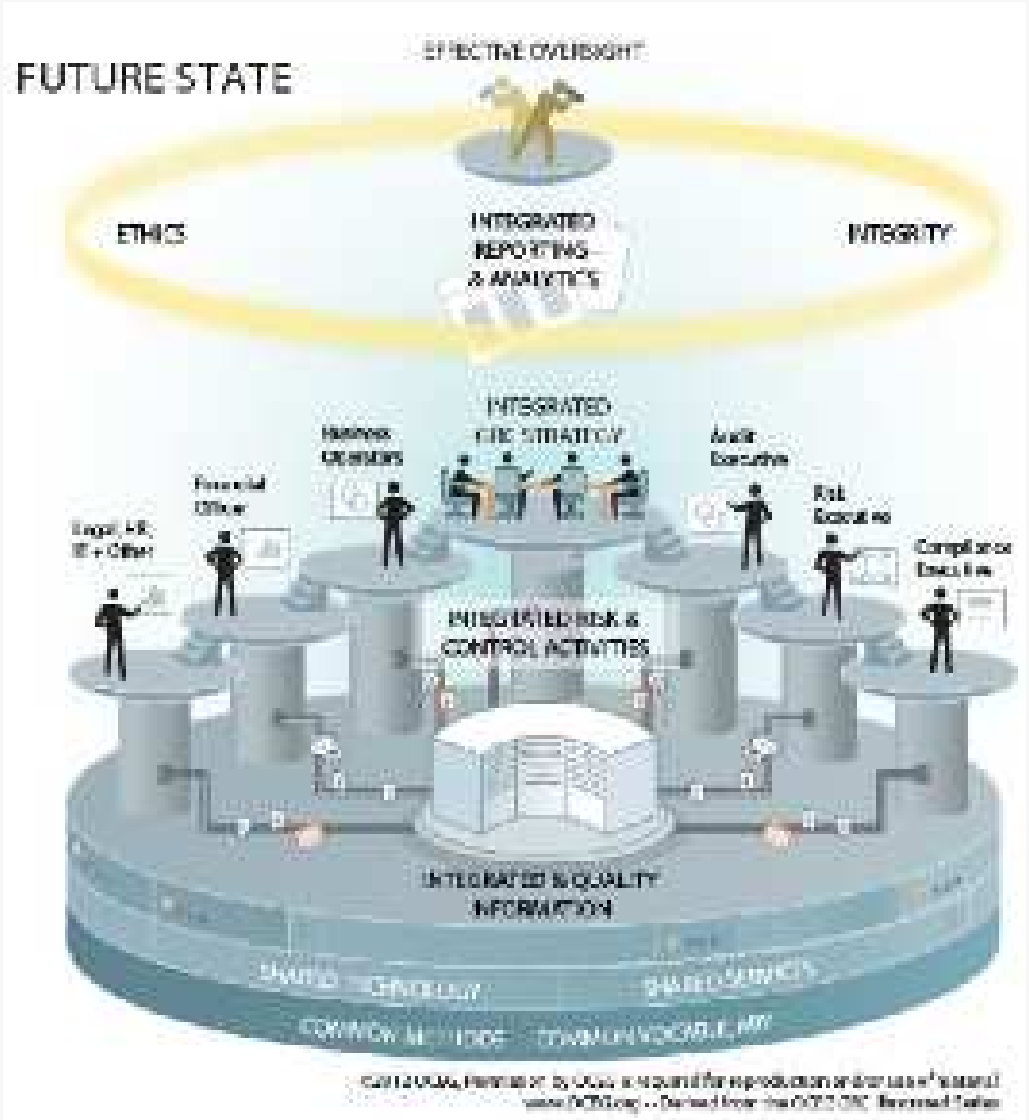
Cyber Strategy

Future State Vision

- Engage key stakeholders and define guiding principles
- Define desired future state
- Identify capability gaps

Future State Vision

- **The Solution**
  - Governance Strategy
  - Risk Management
  - Audit and Internal Audit
  - Compliance, Privacy and Legal



Cyber Strategy

Strategic Roadmap

- Propose new projects
- Identify inter-project dependencies
- Create program roadmap

Phase I: Create Baseline and Risk Identification

2015

Baseline and Identify Risks and Current Exposures

2016

2017

2018

PREVENTION

01

- IT Policies, Standards & Guidelines
- Security Awareness Training

IT POLICY FRAMEWORK

DETECTION

02

- Key Stakeholder Analysis
- Network Assessments
- IT Control Assessments

IT RISK ASSESSMENTS

PROTECTION

03

- IT Control Remediation
- Metrics: Cyber Value-at-Risk (CyVAR)

IT SECURITY GOVERNANCE

Phase II: Convergence of IT Security and IT Operations

2015

2016

Establish Fundamental Security Capabilities

2017

2018

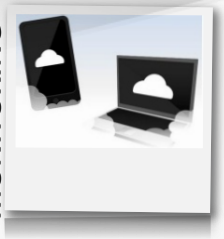
PREVENTION

01

- Content Sharing
- Mobile Devices (MDM)
- Endpoint DLP
- Network DLP
- Network IPS

DETECTION

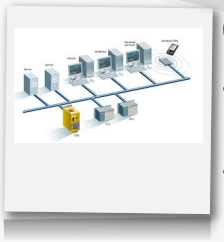
END USER MONITORING



02

- Network IDS
- Security Information & Event Management (SIEM)
- IT Control Self Assessment Process

NETWORK MONITORING



PROTECTION

03

- Endpoint Encryption
- Server DB Encryption
- Oracle Security Assessment

IN-USE
IN-TRANSIT
AT-REST

Phase III: Sustain and Expand Resilient Security Capabilities

2015 | 2016 | **2017** | 2018

2017

Expand Security Capabilities: Defense-in-depth

PREVENTION

01

- Database Scanning
- Secure SDLC

BUILT-IN SECURITY

DETECTION

02

- Digital Forensics
- Cyber Threat Intelligence

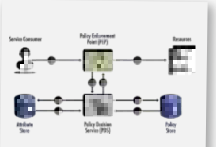
REAL-TIME ASSESSMENT

PROTECTION

03

- Inline Patching
- Web Application Firewall (WAF)

TECHNICAL POLICY ENFORCEMENT



Phase IV: Optimize Security Maturity and Governance

2015 → 2016 → 2017 → **2018**

Operationally Optimized IT Security

PREVENTION

01

- Infrastructure Threat Modeling
- App Dev Threat Modeling

SECURITY BY DESIGN

DETECTION

02

- Network Surveillance
- Web / Mobile Surveillance
- Cloud Surveillance

PERVASIVE PERIMETER DETECTION

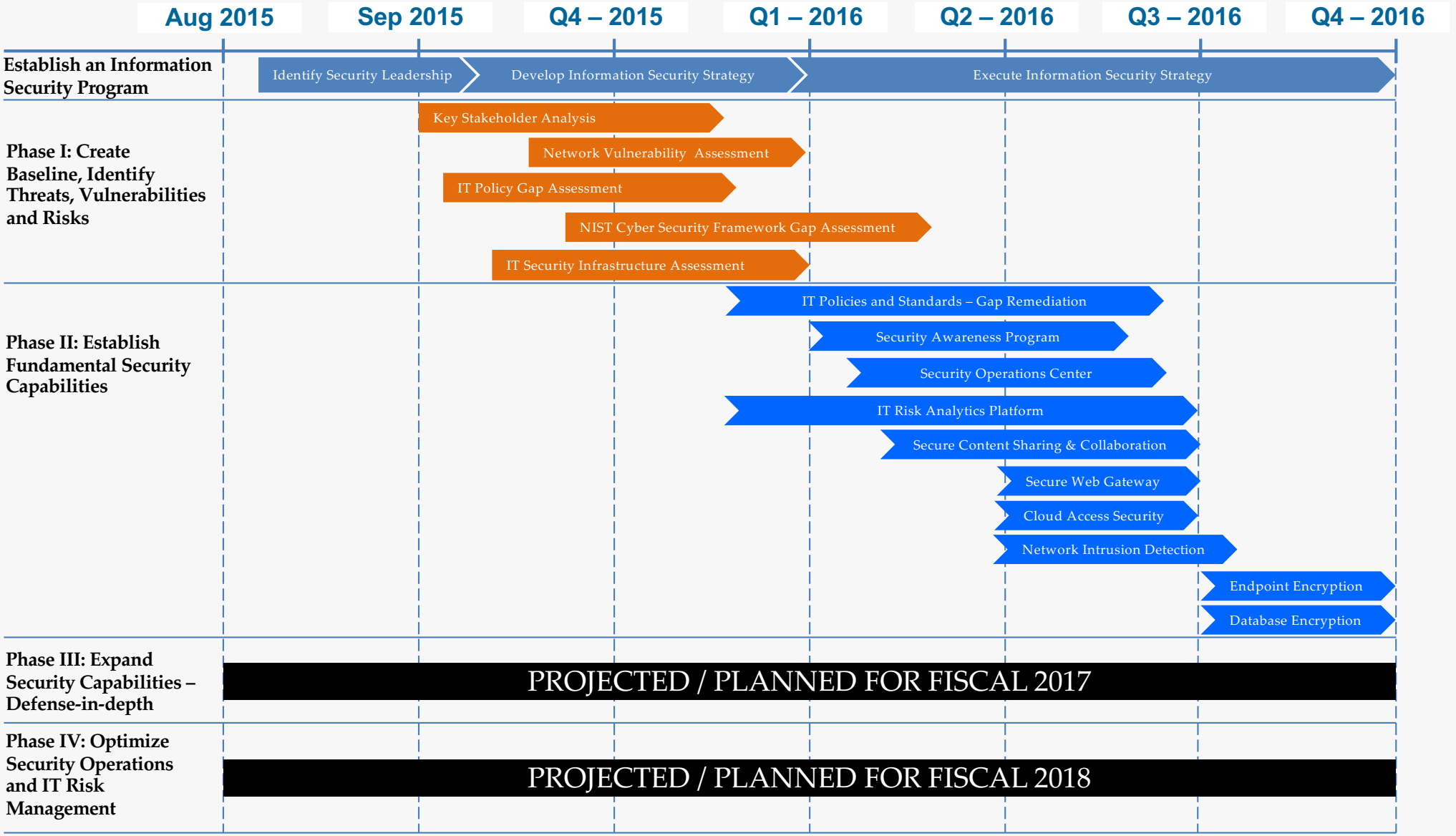
PROTECTION

03

- Process Optimization
- Automation Optimization

DEEP SECURITY PLATFORM

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT



Cyber Strategy

Mobilization

- Plan and execute initiatives and projects
- Communicate progress to key stakeholders

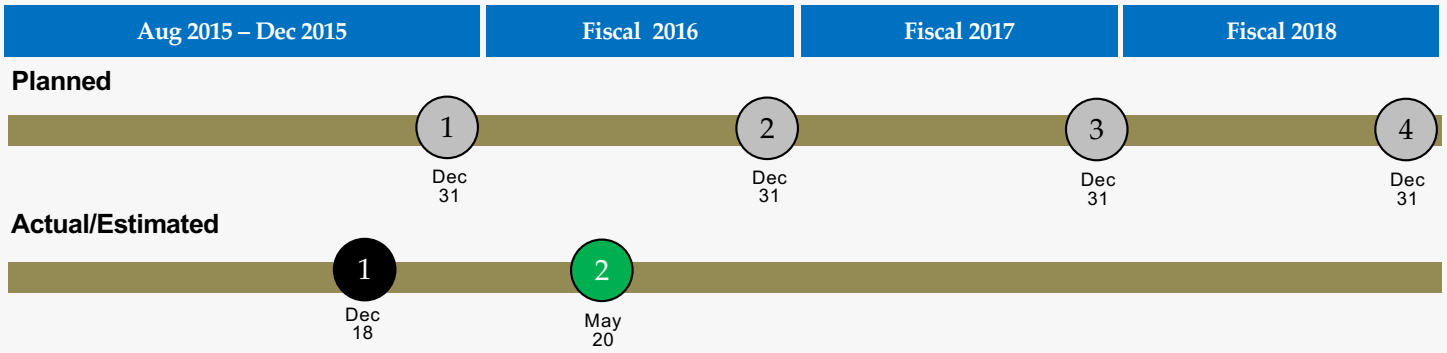
Cyber Strategy

Implementation

- Administrative delivery
- Technical delivery
- Education and training
- Review impact of capabilities

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Timeline



1. **Phase I: Create Baseline and Risk Identification**
2. **Phase II: Establish Fundamental Security Capabilities**
3. **Phase III: Expand Security Capabilities**
4. **Phase IV: Operationally Optimized IT Security**

Q4 – 2015: Accomplishments

- Network Vulnerability Assessment (Penetration Test)
- IT Policy and Standards Gap Assessment
- NIST Cybersecurity Framework Gap Assessment
- Key Stakeholder Analysis
- IT Security Infrastructure Assessment
- 3-Year Information Security Strategy Plan

Q1 – 2016: Accomplishments

- Draft of IT Policies and Standards
- Launch Phase I of Security Awareness Program
- Completed Secure Web Gateway RFP
- Security Operations Center proof of concept (Location X)
- Remediation of Critical Assessment Findings
- IT Risk Analytics Platform: Cyber Value-at-Risk (CyVaR)

Q2 – 2016: In Progress Activities

- Launch Phase II of Security Awareness (Training)
- Launch Pilot of Secure Content Sharing & Collaboration
- Phase I Deployment of Secure Web Gateway (**US IT Operations**)
- Planning Endpoint Security Deployment (Encryption and Host Intrusion Protection - **US only**)
- Phase I Deployment of Security Operations Center (**US IT Operations**)
- Approve and Publish Formal IT Policies and Standards

Q3 – 2016: Projected & Planned Activities

- Launch Phase III of Security Awareness (Phishing)
- Deployment of Endpoint Security (Encryption and Host Intrusion Protection (**US only**)
- Planning for Server Database Encryption
- Phase II Deployment of Secure Operations Center (**International IT Operations**)
- Expand Secure Content Sharing & Collaboration platform
- Phase II Deployment of Secure Web Gateway (**International IT Operations**)

Summary

Our Information Security strategy is designed to position the organization to mitigate, transfer, accept or avoid information security risk related to people, processes and technologies.

This strategy enables the organization to adequately protect the confidentiality, integrity and availability of its information assets.

The primary benefits of the strategy include:

- Compliance with Regulatory Requirements and Industry Standards
- Cost avoidance related to the impact and potential damage associated with the occurrence of security incidents.
- Sustaining the reputation of the business and supporting commitment to shareholders, customers, partners and suppliers.

Gray – Originally planned activity | Green – On track; will complete as planned | Black – Completed activity | Yellow – Planned delivery at risk | Red – Will miss planned delivery

GOLD NUGGET #3

- An overall Cybersecurity Strategy must be **defined**
- A good Cybersecurity Strategy should take a **phased approach**
- Cybersecurity Strategy is iterative and fluid to keep pace with emerging cybersecurity risks

Group Discussion: What's Involved in a Cybersecurity Audit?

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Cybersecurity: What is the role of the Internal Auditor

1. What is the Internal Auditor's role in design or re-design of a Cybersecurity program?
2. How can the Internal Auditor help assess and reduce the risks of a cyber attack?
3. What are the greatest challenges or impediments to the Internal Auditor's role in this effort?

GOLD NUGGET #4

- GTAG – Supplemental Guidance: Assessing Cybersecurity Risk
- Prepared by The IIA, GTAG is written in straightforward business language to address timely issues related to cybersecurity risks
- **HERE'S THE KICKER** – IIA members access GTAG's **FREE**!

Cybersecurity Audit

- **Audit**
  - The process of validating the existence of control mechanisms (administrative and technical), which enforce the established IT security policy.
- **Assessment**
  - The process of validating the effectiveness of control mechanisms (administrative and technical).
  - The simple fact that a control is in place does not mean that it is effective.

Cybersecurity Audit Objectives

- Provide management with an assessment of an organization's cybersecurity controls (administrative, physical and technical) and their operating effectiveness.
- Identify internal control and regulatory deficiencies that could put the organization at risk.

Cybersecurity: What is the role of the Internal Auditor?

What is the Internal Auditor's role in design or re-design of a Cybersecurity program?

- Evaluate and contribute to the improvement of governance, risk management, and control processes
- The internal audit activity plays a crucial role in assessing an organization's cybersecurity risks by considering:
  - Who has access to the organization's most valuable information?
  - Which assets are the likeliest targets for cyberattacks?
  - Which systems would cause the most significant disruption if compromised?
  - Which data, if obtained by unauthorized parties, would cause financial or competitive loss, legal ramifications, or reputational damage to the organization?
  - Is management prepared to react timely if a cybersecurity incident occurred?

First Line of Defense

- **Management (CISO)**
  - **Common first line of defense activities:**
    - Administer security procedures, training, and testing
    - Maintain secure device configurations, up-to-date software, and security patches
    - Deploy intrusion detection systems and conduct penetration testing
    - Securely configure the network to adequately manage and protect network traffic flow
    - Inventory information assets, technology devices, and related software
    - Deploy data protection and loss prevention programs with related monitoring
    - Restrict least-privilege access roles

Second Line of Defense

- **Risk Management – Cybersecurity Committee**
  - **Common second line of defense activities:**
    - Design cybersecurity policies, training, and testing
    - Conduct cyber risk assessments
    - Gather cyber threat intelligence
    - Classify data and design least-privilege access roles
    - Monitor incidents, key risk indicators, and remediation
    - Recruit and retain certified IT risk talent
    - Assess relationships with third parties, suppliers, and service providers
    - Plan/test business continuity, and participate in disaster recovery exercises and tests

Third Line of Defense

- **Internal Audit**
  - As the third line of defense, the internal audit activity plays an important role in coordinating with the second line of defense, particularly the cybersecurity function. The internal audit activity can be consulted regarding:
    - The relationship between cybersecurity and organizational risk.
    - Prioritizing responses and control activities.
    - Auditing for cybersecurity risk mitigation across all relevant facets of the organization; for example, privileged access, network design, vendor management, monitoring, and more

Third Line of Defense

- **Common third line of defense activities:**
  - Provide independent ongoing evaluations of preventive and detective measures related to cybersecurity
  - Evaluate IT assets of users with privileged access for standard security configurations, problematic websites, malicious software, and data exfiltration
  - Track diligence of remediation
  - Conduct cyber risk assessments of service organizations, third parties, and suppliers
    - Note: First and second lines of defense share this ongoing responsibility

ESTABLISHING SCOPE

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Scope and Collaboration

- Scoping for cybersecurity risk is an interdependent exercise that requires internal audit to jointly plan with compliance functions in the second line of defense.
- Audit planning is most effective when integrated with compliance functions who have the insight to prioritize business impact and with whom they can collaborate during and after the internal audit.

Identifying Critical Information

- What information is deemed critical and why?
- What is the value of the data (to fraudsters, competitors, etc.)?
- Where is the information accessed, processed, and stored?
- How is information transmitted?

Identifying Critical Information

- What is the extent of rigor followed to grant and revoke access?
- Have access levels been determined by role and what roles have administrative access?
- How is access assigned, approved, monitored, and removed?
- How well protected is the information to unauthorized access?

Identifying Critical Information

- What type of testing is performed (penetration, access, tracked changes, etc.)?
- How is cybersecurity risk monitored for those who have functional access to critical information?

Approach for Assessing Cybersecurity Risk and Controls

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Cybersecurity Risk Assessment Framework

SOURCE: GTAG – Assessing Cybersecurity Risk and Controls

1. Cybersecurity Governance
   - Effective governance is evidenced in clearly defined policies, relevant tools, sufficient staffing, and insightful training.
2. Inventory of Information Security Assets
   - Preventive and detective controls designed to protect the most valuable assets need to be continuously monitored to ensure ongoing effectiveness.

3. Standard Security Configuration
   - Centralized, automated configuration management software can be used to establish and maintain baselines for devices, operating systems, and application software
4. Information Access Management
   - Management should consider implementing preventive controls such as having a process to approve and grant access to users based on job roles

5. Prompt Response and Remediation
   - The capability of the organization to promptly communicate and remediate risks indicates the program's effectiveness and level of maturity.
6. Ongoing Monitoring
   - As a final component of this assessment framework, continuous auditing of each of the five components described above when conducted will help to determine how risk is managed and how well corrective action is operating.

GOVERNANCE

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Governance

- Strong cybersecurity governance depends on:
  - Collaborating and collecting cybersecurity risk intelligence and expertise based on threats that could affect the organization.
  - Setting risk appetite and tolerance.
  - Planning for business continuity and disaster recovery in the event of an interruption.
  - Responding promptly to security breaches.
  - Establishing a culture of awareness of cybersecurity risks and threats.

Governance

- Here are 10 questions Internal Audit should consider when evaluating the organization's governance related to cybersecurity:
  1. Are senior management and the governing body (audit committee, board of directors, etc.) aware of key risks related to cybersecurity. Do cybersecurity initiatives receive adequate support and priority?
  2. Has management performed a risk assessment to identify assets susceptible to cyber threats or security breaches, and has the potential impact (financial and nonfinancial) been assessed?
  3. Are first and second lines of defense collaborating with their peers in the industry (e.g., conferences, networking forums, and webcasts) to keep current with new/emerging risks, common weaknesses, and cybersecurity breaches associated with cybersecurity?

SOURCE: GTAG – Assessing Cybersecurity Risk and Controls

Governance

4. Are cybersecurity policies and procedures in place, and do employees and contractors receive cybersecurity awareness training on a periodic basis?
5. Are IT processes designed and operating to detect cyber threats? Does management have sufficient monitoring controls in place?
6. Are feedback mechanisms operating to give senior management and the board insight into the status of the organization's cybersecurity programs?

SOURCE: GTAG – Assessing Cybersecurity Risk and Controls

Governance

7. Does management have an effective hotline or emergency procedure in place in the event of a cyberattack or threat? Have these been communicated to employees, contractors, and service providers?
8. Is the internal audit activity capable of assessing processes and controls to mitigate cyber threats, or does the CAE need to consider additional resources with cybersecurity expertise?

SOURCE: GTAG – Assessing Cybersecurity Risk and Controls

Governance

9. Does the organization maintain a list of third-party service providers that have system access, including those that store data externally (e.g., IT providers, cloud storage providers, payment processors)? Has an independent cybersecurity examination engagement been conducted to assess the effectiveness of the service organization's controls as a part of their cybersecurity risk management program?

10. Has internal audit adequately identified common cyber threats facing the organization (e.g., nation-states, cybercriminals, hacktivists, networked systems, cloud providers, suppliers, social media systems, malware), and incorporated these into the internal audit risk assessment and planning processes?

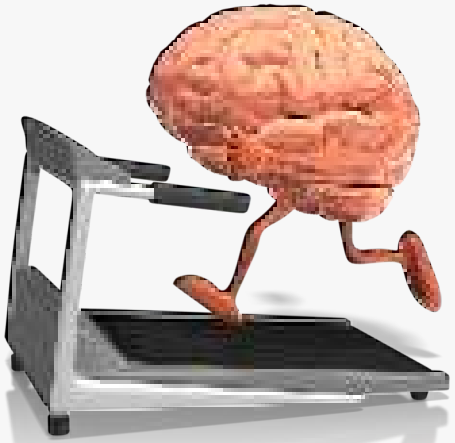
SOURCE: GTAG – Assessing Cybersecurity Risk and Controls

Red Flags, Potential Governance Gaps

- Disparate, fragmented governance structure
- Incomplete strategy
- Delays of cybersecurity effort
- Budget cuts and attrition
- Unclear resolve to enforce accountability

Group Exercise: Cybersecurity Buzzword Bingo

Time Allotted: 20 Minutes



Buzzword Bingo Game

Risk	Weaponize	Next Gen / NGFW	DLP	Phishing
Malware	Recon	IoT	Exploit	Command and Control
CISO	Framework	CYBER SECURITY BUZZWORD BINGO (free square)	Cybersecurity	Intrusion
Blockchain	Exfiltrate	ACL	Kill Chain	NIST
Ransomware	Social Engineering	Hacktivist	Crimeware	Line of Defense

Cybersecurity Controls

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Administrative Controls

- IT security policies and standards relating to the network, database and applications
- User access reviews for general and privileged users
- Separation of duties (development, database administration, implementation, support)
- Security Awareness Training
- Business Continuity / Disaster Recovery Plan
- Hiring practices (qualifications, background checks, etc.)

Physical Security Controls

- Facility Access Control List (ACL)
- Video Surveillance
- Security Guards

Network Security Controls

- Firewall
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Wireless Access Control
- Web and Email Gateways
- Penetration Testing
- Data Loss Prevention (DLP)

Endpoint Security Controls

- Endpoint Detection and Response (EDR)
  - Anti-malware / Anti-virus
- Application Control
- Data Loss Prevention (DLP)
- File Encryption
- Multi-factor Authentication (MFA)
- SSL Certificate
- Vulnerability Assessment

Mobile Security Controls

- Enterprise Mobility Management
  - Mobile Device Management (MDM)
  - Mobile Application Management (MAM)
- Anti-malware / Anti-virus

Cloud Security Controls

- Cloud Access Security Broker
  - Sanctioned vs Unsanctioned cloud apps
- Identity and Access Management (IAM)
  - Single Signon (SSO)
- Configuration Management
- Encryption
  - Data in transit
  - Data at rest

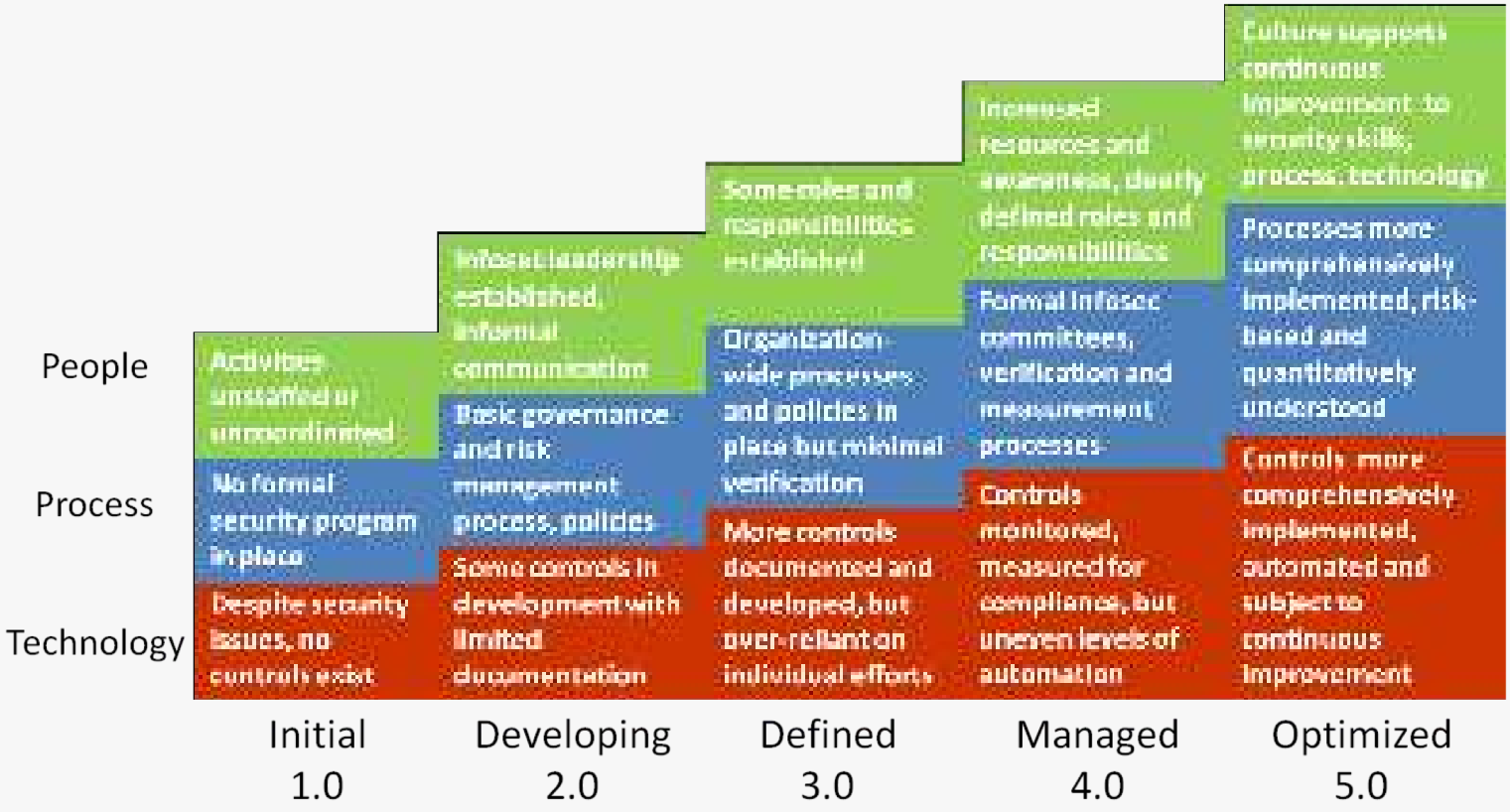
Application Security Controls

- Secure Software Development Lifecycle (SDLC)
  - Security by Design
  - Code Review
  - Static and Dynamic Analysis
- Code Signing

Measuring Cybersecurity Maturity

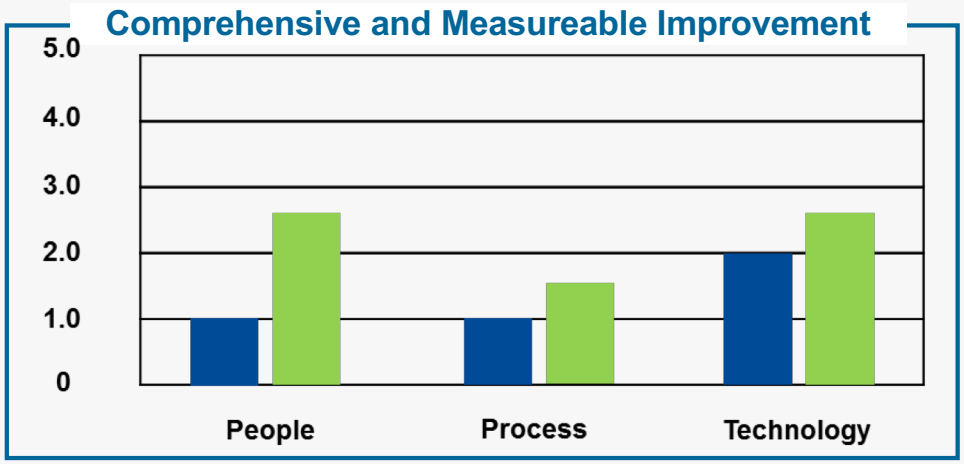
THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

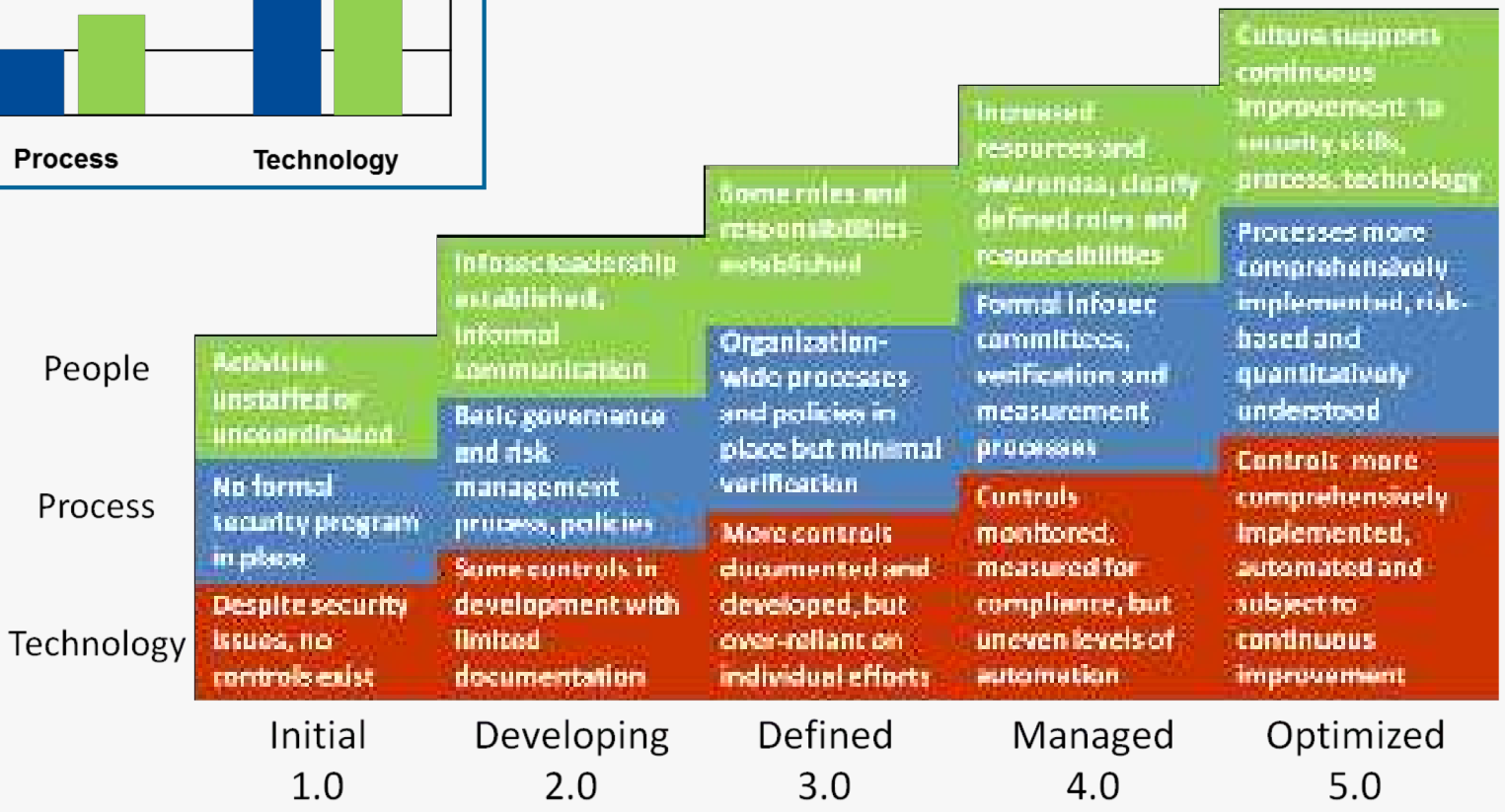
Cybersecurity Maturity Model



SOURCE: Security Architects, LLC: Information Security Maturity Model

Example: Cybersecurity Maturity Model





GOLD NUGGET #5

- Cybersecurity Maturity is a **journey**
- Cybersecurity Maturity must be periodically **measured**
- Cybersecurity Maturity is the **goal**

SUMMARY

THE *STANDARD* IN STAFFING, RECRUITING AND PROFESSIONAL DEVELOPMENT

Gold Nuggets

- Use GTAG Assessing Cybersecurity Risk as a guide
- Cybersecurity Frameworks are Key
- Cybersecurity Strategy is Iterative
- Internal Audit plays a crucial role in assessing an organization's cybersecurity risk
- Cybersecurity Maturity is the Goal

Gold Nuggets – Helpful Links

- NIST Cybersecurity Framework – https://www.nist.gov/cyberframework
- CIS Critical Security Controls Framework - https://www.cisecurity.org/controls/
- Targeted Attack Game - http://targetedattacks.trendmicro.com/
- Mapping the Future: Dealing with Pervasive and Persistent Threats - https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019