Risk Management & Cybersecurity

Course 2002

Chad Tagtow

May 27 - 30

2019 Session
RISK MANAGEMENT & CYBERSECURITY
GSBLSU 2019

INTRODUCTION
WHO AM I?

- Chad Tagtow, CISSP
  Chief Information Officer
  Citizens Bank and Trust
  Lake Wales, Florida

Chad.Tagtow@Citizens-Bank.com

Tagtow@gmail.com

Cell: 863.412.0022

RISK MANAGEMENT AND CYBERSECURITY

- What is Cybersecurity?
  - It is not an IT issue.
  - It is an organizational issue for every size.

- Why is Risk Management such a big deal?
  - Appreciate and understand Risk
  - Risk tolerance
  - Mitigation

- Goal:
  To know enough about the issue to manage it.
  Recognize the Risk...Manage the Risk
EXPONENTIAL INCREASE OF RISK

- Risk is a moving target. Security threats are not static, and experts need to sharpen their judgment calls based on educated guesses about where the greatest risks will be in the future. – Ed Sperling

- Global Cybersecurity Market
  - 2004 - $3.5 Billion
  - 2017 - $120 Billion

BREACH STATISTICS

- 62% Increase in cyber breaches from 2012
- 76% Of Phishing Scams are targeted at financial institutions
- 46% Of intrusions lead to account takeovers

Source: New York State Department of Financial Services
BREACH STATISTICS

24%
Average likelihood of experiencing a breach of 10,000 or more records over a two-year period

BREACH STATISTICS

What are the odds of . . .

Getting struck by lightning?
1 in 960,000

Dating a millionaire?
1 in 220

Experiencing a data breach?
1 in 4

(Global average 28%)
BREACH STATISTICS

- Chili's – May 2018
- SunTrust – 1,500,000 – April 2018
- Orbitz (Expedia subsidiary) – 880,000 – March 2018
- FedEx / Bongo – 119,000 – Feb 2018
- Jason's Deli – Dec 2017 – 2 Million
- Equifax – 147.9 million – Sept 2017
- MICROS – 2016 - 330,000 cash registers
### BREACH STATISTICS

**Identity Theft Resource Center 2017 Data Breach Industry Summary**

<table>
<thead>
<tr>
<th>Totals for Category</th>
<th># of Breaches</th>
<th>% of Breaches</th>
<th># of Records</th>
<th>% of Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking/Credit/Financial</td>
<td>134</td>
<td>8.6%</td>
<td>3,122,090</td>
<td>1.7%</td>
</tr>
<tr>
<td>Business</td>
<td>878</td>
<td>66.1%</td>
<td>163,449,242</td>
<td>91.3%</td>
</tr>
<tr>
<td>Educational</td>
<td>127</td>
<td>8.0%</td>
<td>1,416,250</td>
<td>0.8%</td>
</tr>
<tr>
<td>Government/Military</td>
<td>74</td>
<td>4.7%</td>
<td>5,963,448</td>
<td>3.2%</td>
</tr>
<tr>
<td>Medical/Healthcare</td>
<td>374</td>
<td>23.7%</td>
<td>5,062,031</td>
<td>2.8%</td>
</tr>
</tbody>
</table>

**Totals for All Categories:**

- # of Breaches: 1,879
- # of Records: 178,885,069

---

**BREACH STATISTICS**

Key finding: the cost of a data breach continues to rise

<table>
<thead>
<tr>
<th>Cost per record</th>
<th>Cost per incident</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global average</strong></td>
<td><strong>Global average</strong></td>
</tr>
<tr>
<td><strong>$158</strong></td>
<td><strong>$4M</strong></td>
</tr>
<tr>
<td>$158</td>
<td>$4M</td>
</tr>
</tbody>
</table>

**15% since 2013**

**29% since 2013**

<table>
<thead>
<tr>
<th>Highest countries</th>
<th>Lowest countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>$221</td>
<td>$100</td>
</tr>
<tr>
<td>$213</td>
<td>$61</td>
</tr>
<tr>
<td>UNITED STATES</td>
<td>BRAZIL</td>
</tr>
<tr>
<td>GERMANY</td>
<td>INDIA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Highest countries</th>
<th>Lowest countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>$7M</td>
<td>$1.8M</td>
</tr>
<tr>
<td>$5M</td>
<td>$1.6M</td>
</tr>
<tr>
<td>UNITED STATES</td>
<td>SOUTH AFRICA</td>
</tr>
<tr>
<td>GERMANY</td>
<td>INDIA</td>
</tr>
</tbody>
</table>
BREACH STATISTICS

The largest component of the total cost of a data breach is lost business.

- Lost business cost: $1.63 million
- Detection and escalation: $1.09 million
- Ex-post response: $1.10 million
- Notification: $0.18 million

Components of the $4 million cost per data breach:
- Abnormal turnover of customers, increased customer acquisition cost
- Reputation losses, diminished goodwill
- Forensics, root cause determination, organizing incident response team, identifying victims
- Disclosure of data breach to victims and regulators

Currencies converted to US dollars.

BREACH STATISTICS

The per-record cost of a data breach varies widely by industry:

- Healthcare: $355
- Education: $246
- Financial: $221
- Services: $208
- Life science: $195
- Retail: $172
- Communications: $164
- Industrial: $150
- Energy: $146
- Technology: $145
- Hospitality: $139
- Consumer: $123
- Media: $113
- Transportation: $109
- Research: $103
- Public: $90

Average cost per record breached.

Healthcare and finance experienced larger costs.

Currencies converted to US dollars.
RISK LANDSCAPE

- Welcome to the Wild West!
  - Bandits, Cholera, Snake bites, Dysentery
  - Hackers, Viruses, Spyware, Adware, Keystroke loggers
  - ATM skimmers, ATM jackpotting, Denial of Service
  - Phishing, Botnets, Advanced Persistent Threats
  - Corporate Account Takeover

- There is little to no policing, you have to protect yourself!

- If you aren't prepared...

CONSEQUENCES

You have died of dysentery.
MANAGING RISK

PRINCIPLES OF RISK

- **Risk**: The potential for loss, damage or destruction of an asset

- The people who manage risk the best WIN

- No risk, no reward
TYPES OF RISK

- Financial Risk
- Operational Risk
- Strategic Risk
- Regulatory / Legal Risk
- Reputational Risk

RISK MANAGEMENT STRATEGIES

- Limit Risk
- Avoid Risk
- Assign Risk
- Informed Acceptance of Risk
RISK STRATEGY - LIMIT RISK

• Limit Risk – Most common risk management strategy
  • Reduce the likelihood and/or impact of the risk
  • Detection, deterrence, prevention

• Examples:
  • Virus/Malware protection software
  • Web filtering, Firewalls, Patching, Intrusion Detection Systems
  • Larger down payment
  • Increase collateral
  • Personal guarantees
  • Annual credit reviews

RISK STRATEGY - AVOID RISK

• Avoid Risk – Likely the most expensive risk strategy
  • Avoid the business activity to avoid the risk
  • Not start or continue with activity that gives rise to the risk

• Examples
  • No internet banking
  • No mobile app / check deposit
  • No email for the whole bank
  • No fixed rate loans
  • No loans with below 800 credit
  • No commercial loans
RISK STRATEGY - ASSIGN RISK

- Assign Risk – Pay to assign risk to willing third party
  - Sharing the risk with another party
  - Contracts with vendors
  - Risk Financing - Insurance

- Examples
  - Insurance (cyber, home, fire, car)
  - Payroll services, data processing, etc
    - Areas of operation that are not a core competency

RISK STRATEGY - ACCEPTANCE

- Informed Acceptance of Risk
  - Retaining the risk by informed decision
  - Clearly defined, understood, and communicated
  - Risk expense vs opportunity analysis

- Examples
  - No insurance / self insurance
    - 100 year flood zone
  - Cost of risk management outweighs the cost of the risk
  - Small investment with big longshot reward
COMPONENTS OF RISK

- Threats
- Vulnerabilities
- Likelihood
- Impact
- Mitigations

THREATS

- **Threat**: A potential cause of an incident, that may result in harm of systems and organization

- Examples of THREATS:
  - Hacker
  - Theft
  - Inadequately trained staff (accidental)
  - Hurricane
  - Fire
  - Lightning Strike
VULNERABILITIES

- **Vulnerability**: A weakness in design, implementation, operation or internal control

- Examples of VULNERABILITIES:
  - Software bug
  - Hardware prone to failure
  - Data Center located on the coast in a flood zone
  - Unencrypted communication
  - No checklist for important control

RISK ASSESSMENT PROCESS
LIKELIHOOD

- Likelihood: Likelihood refers to the possibility of a threat event occurring measured in qualitative values such as Low, Medium, or High.

- Probability: Percentage of possibility of a threat event occurring measured in a quantitative value such as 80%.

IMPACT

- Impact: The loss, damage, or destruction of an asset. This severity is based on the Business Criticality of the asset.
- Impact = Loss x Business Criticality of Asset
- Business Criticality – This should represent the importance of the asset to the business.

- Qualitative or Quantitative
## IMPACT LOSS

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
</table>
| 5 Severe/Critical | Asset will be lost, or critical objective(s) will fail                     | 10 Million loss
|           |                                                                             | 10% of net income                                                     |
| 4 Significant/High | Asset performance will be significantly reduced, or objectives will fall below acceptable levels | Bank is under a MOU with regular reporting to regulators |
| 3 Moderate/Medium | Asset performance will be moderately reduced, or objectives will fall well below goals but above minimum levels | <3000 customers affected negatively |
| 2 Low     | Asset performance will be reduced, objective will fall below goal but still acceptable | <$5000 loss |
| 1 Minimal | Minimal impact on asset, performance below optimal | Statement mailing delayed by 1 day |

## RISK ASSESSMENT PROCESS

1. **Risk Identification**
2. **Assess Residual Risks**
3. **Risk Analysis**
4. **Risk Mitigation**

Inherent Risk = (Threat x Vulnerability x Impact)
MITIGATIONS

- Mitigations: Controls or processes that
  
- Reduce impact
  - Less records exposed, insurance coverage, UPS backup

- Reduce likelihood/probability of threat event
  - Move data center away from coastal Miami, Police guard

- Remove vulnerability
  - Patch servers, Tier 1 hardware, encrypt communications

RISK ASSESSMENT PROCESS
RISK

- **Inherent Risk**
  - Risk = (threat x vulnerabilities x likelihood x impact)

- **Residual Risk**
  - Residual Risk = Inherent Risk – Mitigating Controls
  - Or
  - RR = Mitigated (threat x vuln x likelihood x impact)

- Example: Data Center

RISK

- Data Center – Business Criticality (scale of 0-10) **10**
- Threat = Hurricane (Critical 5) **5**
- Vulnerability = Located on Florida coast (Critical 5) **5**
- Likelihood = (Minimal 1) **1**
- Impact = Critical objectives fail (Critical 5) = 10 x 5 = **50**

- Risk = (5 x 5 x 1 x 50) Inherent Risk = 1250
- Mitigating Control = Move Data Center to Arizona
- Residual Risk = Inherent Risk – Mitigating Controls
- Residual Risk = 1250-1250 = 0
- RR = (5 x 5x 0 x 50) = 0
RISK

- Servers – Business Criticality – (10)
- Threat = System Failure - Overheating (High 4)
- Vulnerability = A/C units are 12 years old (Med 3)
- Likelihood = 2.5 (low to moderate)
- Impact = Critical objectives fail (Severe 5)

Risk = (4 x 4 x 2.5 x 5) = 320
Inherent Risk = 320

Mitigating Control = Replace AC units
Residual Risk = Inherent Risk – Mitigating Controls
Residual Risk = (4 x 4 x 1 x 5) = 80

RISK (QUANTITATIVE)

- Servers – Business Criticality – (Critical 5)
- Impact of VulnThreat = System Failure - $150k
- Probability of event = 48%
- Inherent Risk = Threat x Vuln x Impact x Prob
  Inherent Risk = $72k

- Mitigating Control Cost = Replace AC units $35k
- Mitigated Likelihood of Threat event = 7%
- Residual Risk = Mitigated(Inherent Risk)
- Residual Risk = ($150k x 7%) = $10,500
QUALITATIVE OR QUANTITATIVE?

- Which is better Qualitative or Quantitative?

- Qualitative
  - Expensive and time consuming to assign $ figures to every asset, percentages for every threat, $ effectiveness to every control.

- Quantitative
  - You can't improve what you can't measure

RISK APPETITE
RISK APPETITE

- Risk Appetite – Risk Tolerance
  - The amount and type of risk that an organization is willing to take in order to meet their strategic objectives.
  - This will likely be different for every asset and type of risk
    - Loans in 2007
    - Irrational exuberance
    - Overdraft losses
    - Appetite for some types of risk and averse to others
  - Risk Appetite is based upon the Residual Risk.
  - How much unmitigated (residual) risk is the institution willing to accept.

RISK APPETITE

- Risk appetite approaches
  - **Risk Averse** – avoid risk, ultra safe option, low risk low reward
    - Operational people

  - **Risk Neutral** – handled on a case by case basis

  - **Risk Seeker** – Early adopter, innovative, high risk high reward
    - Executives
RISK APPETITE

- The bank must have a cyber risk appetite statement approved by the board or an appropriate board committee.
- This should be asset by asset, but it can be risk type by risk type.
- Can be Quantitative ($) or Qualitative (1-10, H,M,L)
  - Financial Risk – Medium 3-5
  - Operational Risk – Medium 5-6
  - Reputational Risk – Low 1-3
  - Regulatory Risk – Low 2-4

RISK MANAGEMENT

- Risk Management is split into three categories:
  - Risk Taker (Board of Directors)
  - Risk Controller (Risk Management)
  - Independent Assurance (Audit)
RISK MITIGATION

CURRENT SPEND

- Where are you spending your Risk Mitigation money?
- Why are spending that amount?
- Why in those areas?
POTENTIAL LOSS

- What is the potential loss?

- Regulatory Risk
  - Exam rating of "2". Don’t overspend. Don’t get in trouble.

- Risk Management
  - Adequately protect to threat independent of regulations

HOW MUCH AND WHERE DO I SPEND?

- Calculus of Negligence (Rule of Hand)
- $P =$ probability of event
- $L =$ $ of loss
- $B =$ $ of security investment

![Expected Loss vs Security Investment](chart.png)
HOW MUCH AND WHERE DO I SPEND?

- Where should we spend?

- Money and resources should be applied to two main areas:
  - The areas of highest Residual Risk
  - The areas that have the largest gap between the Residual Risk and the Risk Appetite.
CONFIDENTIALITY

- Confidentiality - information is not made available or disclosed to unauthorized individuals, entities, or processes

- Examples:
  - Stolen Data
  - Unauthorized access to database (breach)
  - Email sent with customer data to wrong person
  - Laptop stolen
  - Statement mailed to wrong address
  - ATM skimmer
INTEGRITY

- Integrity - maintaining and assuring the accuracy and completeness of data over its entire lifecycle

- Examples:
  - Website Defacement
  - Who has access to make changes to data?
  - I just changed my account balance to $1 Million
  - Sabotage by changing data
  - Round fraction of penny into my account

AVAILABILITY

- Availability – Access to data or systems when needed

- Examples:
  - Denial of Service Attack
  - Hurricane floods your data center
  - Hardware failure
  - Ransomware
  - Security control
DEFENSE IN DEPTH

- Layered Security Approach is the only way to mitigate risk.
- In the event one layer is breached, there are multiple layers still protecting the asset.

SANS CRITICAL SECURITY CONTROLS

1. Inventory of Authorized & Unauthorized Devices
2. Inventory of Authorized & Unauthorized Software
3. Secure Configurations for Hardware & Software
4. Continuous Vulnerability Assessment & Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, & Analysis of Audit Logs
7. Email & Web Browser Protections
8. Malware Defenses
9. Limitation & Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring & Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response & Management
20. Penetration Tests & Red Team Exercises
CYBER-INSURANCE

CONSIDERATIONS

- Types
  - Data Breach Liability – Unauthorized disclosure of data
  - Electronic Funds Transfer Fraud
  - Cyber Liability – DOS, Phishing, Virus, Network Breach
  - Cyber Publishing & Social Networking Liability
  - Regulatory Defense
  - Breach Response Expenses
  - PR Expenses
  - Business Interruption
  - Extortion
  - Debit Card Fraud
CONSIDERATIONS

• Policy Amounts and Coverage
  • How much insurance should you have?
  • Let’s assume worst case scenario
  • (Total number of records) × Avg cost per record = loss
  • 20,000 × $221 = $4,420,000

• What is likelihood of breach?
  • Worst case worldwide 28%
  • Banks breached in 2017 ~ 134
  • Total FDIC banks in USA ~ 5600
  • Likelihood you will be breached ~ 1 in 40

VENDOR MANAGEMENT
DUE DILIGENCE

- Must perform due diligence before contract
- New vendor may introduce new or different risks
- Determine Vendor Criticality

VENDOR CRITICALITY

- How do you determine if a vendor is Critical?
- Has access to critical company data?
- Performs one or more "critical" business functions
- Has access to sensitive/confidential data
- Has direct impact on revenue or expenses
- Directly impacts your ability to perform a critical business function
- Great difficulty in replacing vendor.
DUE DILIGENCE

- Critical Vendors / Third-party Service Providers (TSPs)
- Business continuity program
- Financial Condition
- IT Program and Controls
  - Understand the due diligence process the TSP uses for its subcontractors and service providers
  - Incident Response
  - SSAE 16/18

SSAE 16

- SSAE16 Service Org Control Audit
- SOC1, SOC2, SOC3
- Type 1 or Type 2

<table>
<thead>
<tr>
<th>SOC 1</th>
<th>Report on controls for Financial Statement audits</th>
<th>Restricted Use Report (Type 1 or 2)</th>
<th>Auditor judgment for relevance &amp; materiality</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC 2</td>
<td>Report on controls related to compliance or operations</td>
<td></td>
<td>Trust Services Principles &amp; Criteria Apply</td>
</tr>
<tr>
<td>SOC 3</td>
<td></td>
<td>General Use Report (w/Public Seal)</td>
<td></td>
</tr>
</tbody>
</table>
SOC 1

- **SOC1** – basically the same as the old SAS 70
  - It deals with controls for service org that impact control over financial reporting
  - It does not address controls they use to process our data

- **Type 1** – Report on management’s description of system and controls as of a specified date
- **Type 2** – Report on management’s description of system and control over a specified time period

SOC 2

- **SOC2** – Report on controls at service organization that holds, stores, or processes information of the bank.
  - Confidential data, customer data, PII, etc.
  - Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality or Privacy.
  - This is the one you want!

- **Type 1** – point in time snapshot
- **Type 2** – over a specified time period
SSAE 16

- What to look for...
  - Scope? What is being tested? What systems?
  - What date/dates? Type 1/Type 2
  - Management's Assertion
  - Description & Tests of Controls and Results of Tests
  - "In our opinion" – Controls in place, designed to provide...Trust Services Criteria
  - Complementary User Entity Controls
    - Recommend documenting meeting these controls

CONTRACTS

- Things that should be in the critical TSP’s contract:
  - Right to audit
  - SLAs, RTO, RPO – Tie to Default and termination
  - BCP testing
  - Data governance: ownership and handling of data
  - Security issues: Incident response, breach notification
MONITORING

- Periodic assessments of:
  - TSP's control environment
  - Service Level Agreements
  - Business Continuity Plan Test results
  - Financial condition

LAW AND REGULATIONS
GLBA

• Gramm-Leach-Bliley Act of 1999

• Ensure the security and **confidentiality** of customer information;
• Protect against any anticipated threats or hazards to the security or **integrity** of such information; and
• Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

GLBA

• Identifying and assessing the risks that may threaten consumer information

• Developing a written plan containing policies and procedures to manage and control these risks;

• Adjusting the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security.
APPENDIX B - PART 364

- Development of Information Security Program
- Involve Board of Directors
- Assess Risk
- Manage and Control Risk
- Oversee Service Provider Arrangements
- Adjust the Program
- Report to the Board

- Incident Response Program

- Customer Notification

FFIEC

- Federal Financial Institutions Examination Council

- Interagency body to set uniform standards for the federal examination of financial institutions.

- FRB – Federal Reserve System
- FDIC – Federal Deposit Insurance Corp
- NCUA – National Credit Union Administration
- OCC – Office of the Comptroller of the Currency
- CFPB – Consumer Financial Protection Bureau
- CSBS – Conference of State Bank Supervisors
FDIC FIL

- Financial Institution Letters (FILs) may announce
- new regulations and policies,
- new FDIC publications, and
- a variety of other matters of principal interest to those responsible for operating a bank or savings association.

OCC & FEDERAL RESERVE

- OCC issues specific guidance to OCC-supervised banks through Bulletins
- Federal Reserve issues specific guidance to institutions supervised by them in the form of Supervision and Regulation Letters.
BUSINESS CONTINUITY PLAN

BUSINESS IMPACT ANALYSIS

- The BIA drives the entire BCP. If you don't have a BIA you don't have a BCP. It is the first step.

- Identify the potential impact of business disruptions on functions and processes.

- Estimate maximum allowable downtime

- Estimate Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)
CRITICAL SYSTEMS

• Critical System is defined as a system, function, or asset, whether physical or virtual, that is so vital that the incapacity or destruction of such may have a debilitating impact.

• RTO – The maximum allowable downtime that can occur without severely impacting the bank.

• RPO – The amount of data that can be lost without severely impacting the bank.

• Business Continuity Plans should be tested at least annually.

CRITICAL SYSTEMS

• Examples:
  • Wire transfer / Fed funds settlement
  • Cash Letter transmission
  • Cash check
  • Take loan app
  • Process loan
  • File Call Report
INCIDENT RESPONSE

- Not IF, but WHEN - What will you do to prepare? How will you respond?

- Incident Response Plan
  - Periodically Tested
  - Scenario planning, tabletop testing

- Plan should define thresholds for incidents

- When do you notify the regulators, customers?
INCIDENT RESPONSE

- Public Relations Strategy
- Message Content
- When to say what
- Delivery Channels
- Allocation of Staffing

INCIDENT RESPONSE

- **Containment** – primary purpose is to limit the damage.
  - The first step is Short-term Containment.
  - Don’t power off. **Unplug the network cable.**

- **Evidence Protection** – It may be necessary to capture a forensic image of the affected system. This can be used for legal action, or lessons learned.
INCIDENT RESPONSE

- **Eradication** – The removal of any malicious software and the restorations of affected systems. Usually, this is a reimaging of the system’s hard drive.

- **Recovery** – Bring system back into production environment.

AUDIT / COMPLIANCE
VULNERABILITY ASSESSMENT

- Why have a Vulnerability Assessment?
- Who should perform the VA?
- What type of VA?
  - Network Based
  - Host-Based
  - Application
- How often should we have a VA?

PENETRATION TESTING

- Why have a Penetration Test?
- Who should perform the PenTest?
- What type of Pen Test?
  - Network
  - Client-side
  - Web application
  - Social engineering
- How often should we have a Pen Test?
FFIEC CYBERSECURITY ASSESSMENT TOOL

FFIEC - CAT

- Introduced in June of 2015 as a voluntary tool to help financial institutions’ management identify risk and determine their cybersecurity preparedness

- Repeatable measurable process

- Use of the tool is VOLUNTARY

- Two Parts:
  - Inherent Risk Profile and Cybersecurity Maturity
FFIEC - CAT

- **Inherent Risk Profile:**
  - Technologies and Connection Types
  - Delivery Channels
  - Online/Mobile Products and Technology Services
  - Organizational Characteristics
  - External Threats

- **Inherent Risk Levels:**
  - Least, Minimal, Moderate, Significant, Most

---

FFIEC - CAT

- **Cybersecurity Maturity Level: 5 Domains**
  - 1. Cyber Risk Management and Oversight
  - 2. Threat Intelligence and Collaboration
  - 3. Cybersecurity Controls
  - 4. External Dependency Management
  - 5. Cyber Incident Management and Resilience
### Table 3: Risk/Maturity Relationship

<table>
<thead>
<tr>
<th>Cybersecurity Maturity Level for Each Domain</th>
<th>Inherent Risk Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Innovative</td>
<td>Least</td>
</tr>
<tr>
<td>Advanced</td>
<td></td>
</tr>
<tr>
<td>Intermediate</td>
<td></td>
</tr>
<tr>
<td>Evolving</td>
<td></td>
</tr>
<tr>
<td>Baseline</td>
<td></td>
</tr>
</tbody>
</table>

**EMERGING THREATS**
EMERGING THREATS

• New technologies  New products  New risks

• Risk Assessment and Planning (FFIEC)
  • Marketplace conditions.  Customer demographics.
  • Technology standards.
  • Regulatory requirements (e.g., privacy, security, consumer disclosures, and other reporting requirements).
  • Cost containment.
  • Process improvement and efficiency gains.
  • Third-party relationship opportunities versus in-house expertise.

EMERGING THREATS

• Emerging Payment Technologies

• Contactless Cards – RFID

• Proximity Payments – Mobile phone
  • Infrared
  • RFID
  • NFC
  • Bluetooth

• Biometrics
CYBERSECURITY

THREATS

- Hackers
- Ransomware
- Mining Cryptocurrencies
- Phishing / Spear Phishing
- Advanced Persistent Threat
- Corporate Account Takeover
- ATM compromise
- DDoS
- Social Engineering
BREACHES

95% of all successful cyber attacks is caused by human error.

DON'T BE A VICTIM OF A CYBERHEIST

ALWAYS LOCK YOUR WORKSTATIONS

75M PHISHING SCAM EMAILS ARE SENT EVERY DAY

NEVER INSERT AN UNKNOWN USB STICK IN YOUR COMPUTER

NEVER USE A POST-IT NOTE FOR STORING YOUR PASSWORDS

NEVER OPEN EMAIL ATTACHMENTS YOU DIDN'T ASK FOR

91% OF SUCCESSFUL DATA BREACHES STARTED WITH A SPAM PHISHING ATTACK

9 OF 10 PHISHING EMAILS ARE NOW RANSOMWARE

4,000 CYBER ATTACKS OCCUR EVERY DAY

$2.3B OF THE ESTIMATED ANNUAL COST OF GLOBAL RANSOMWARE

MAKE SURE YOU ARE USING A HTTPS CONNECTION WHEN USING A CREDIT CARD TRANSACTION
SOCIAL ENGINEERING

- Social Engineering exploits the human weakness.
- Pretexting
- USB
- Dumpster Diving
- Phishing

Phishing

WHAT YOU NEED TO KNOW

SCAMMERS ARE AFTER YOUR

Passwords  Financial Info  Identity  Money

WHY DO WE FALL FOR THESE SCAMS?

- Urgency
- Desire to please
- Greed
- Curiosity
- Complacency
- Fear

PROBABILITY THAT A PHISHING MESSAGE SUCCEEDS

1 out of 10!
PHISHING

• According to a new report from PhishMe that found that 91% of cyberattacks start with a phish

• Top reasons people are duped by phishing emails:
  • Curiosity (13.7%)
  • Fear (13.4%)
  • Urgency (13.2%)
  • Followed by reward/recognition, social, entertainment, and opportunity.

• Only 50% of employees receive initial cyber training.
PHISHING

- Phishing Training resources:
- KnowBe4
- Cofense (Phishme)
- Wombat
- SANS

- Other Defenses:
- Mail Proxy with sandboxing
- Firewall
- Web Proxy

BREACHES

- Most breaches occur because of Phishing or Social Engineering.

- How do you mitigate this risk?
- Two Factor Authentication
- Malware Protection Software / AV
- Diligent Patching
- Intrusion Detection Software / Heuristic
- Logging
- Insurance
- Monitoring / Intrusion Prevention
- Training
RANSOMWARE

- Ransomware is one of the most popular payloads for Phishing.
- Once it is installed, it will encrypt your data. They will threaten to publish data or keep it locked forever, unless you pay an amount in return for the key to unlock your files.
- Prices range from $300-$1000 for a single PC
- For larger companies, the sweet spot is around $50k
- Ransomware Damage
  - 2017 - $5 Billion
  - 2019 estimate - $11.5 Billion

RANSOMWARE

- The city of Atlanta spent more than $2.6 million on emergency efforts to respond to a ransomware attack that destabilized municipal operations last month. Attackers, who infected the city's systems with the pernicious SamSam malware, asked for a ransom of roughly $50,000 worth of bitcoin.

- Hancock Health has paid hackers $55,000 to unlock systems following a ransomware infection.
ADVANCED PERSISTENT THREAT

- APT – a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time in order to steal data, rather than cause damage to the org.

- Average time to discovery: 8 months

CORPORATE ACCOUNT TAKEOVER

- 43% of cyber attacks target small business
- 70% lack basic security controls
- ACH and Wire Fraud

- FFIEC guidance on CATO
- Layered security controls
- Two factor authentication
- Device identification
- Customer and employee awareness
CLOUD SECURITY

- What is the cloud?
  - Security of the cloud
    - Who is responsible for what?
  - Security in the cloud
    - Who is responsible for what?

CLOUD SECURITY

[Diagram showing responsibilities of AWS and customers in cloud security]
PEOPLE

- Set the tone from the top. (Board, C-suite)
- Create a culture of Risk Awareness
  - Employees & Customer Awareness
- Employ qualified people with the right attitude
- Train and test your people
- Communicate the bottom-line impact of security decisions on your organization to the Board

PROCESS

- Formalized and well documented processes
  - Communicate and Train
- Governance Frameworks
  - NIST, ISO 27001, COBIT
- Processes should align to Risk Management Goals (Business Goals & Security Goals)
TECHNOLOGY

- Every technology solution is dependent upon competent trained people following well defined processes.