

CYBER SECURITY

Updates, Trends, and Recommendations

November 7, 2017

Introduction



Kevin Carpenter

Director, Risk Advisory Services
Kevin.Carpenter@rsmus.com
(513) 354-3503

- IT Risk and Security & Privacy Focused
 - Penetration Testing
 - Vulnerability Assessments
 - Security Monitoring
 - Digital Forensics & Incident Response
 - Controls Assessments
 - Governance Maturity Assessments

Agenda

- Security Statistics
 - Current trends from a cybersecurity and associated risk perspective
- Threat Updates
 - Impact a breach can have on your business
- Recommendations
 - Best practices and strategies to help mitigate and prepare

**Attempting to stay as non-technical as possible*

SECURITY STATISTICS

Security Statistics

Quick Hits

Compiled from:
- NetDiligence/RSM Annual Cyber Claims Study

KEY FINDINGS

Breaches are not just for the Fortune 500 companies anymore.

The majority (87%) of claims submitted for this study are for organizations with revenues less than \$2B.

The numbers of records lost can be large, no matter how large or small an organization may be.

Our dataset contains breaches of 1M or more records occurring in organizations of all sizes, except Mega Revenue (>\$100B).

Breaches can be very costly, no matter how large or small an organization may be.

In our dataset, breaches with total costs greater than \$5M occurred in organizations of all sizes except Mid Rev (\$2–10B).

Breaches with few records can be very costly. One event in our dataset involved 1 record (PHI) with a cost of between \$1.5–2.0M.

The average number of records lost was 2.04 million. The median number of records lost was 1,339.

The greatest numbers of exposed records occurred in the Financial Services (78M records) sector, followed by Retail (56M records).

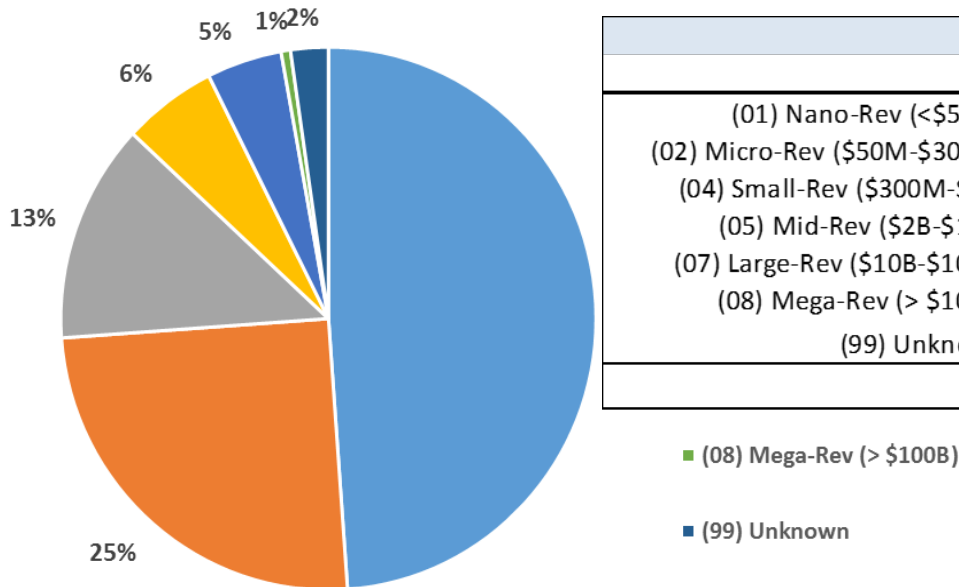
Security Statistics

Compiled from:
- NetDiligence/RSM Annual Cyber Claims Study

- Organization Size

The largest legal costs were from Micro-Revenue organizations. The largest regulatory costs were from the actions of a rogue employee at a Mega-Revenue organization.

Percentages of Claims by Revenue Size
(N = 176)



| | Total Costs (including SIR) | | | | |
|-------------------------------|-----------------------------|------------|------------|------------|------------|
| | Cases | Min | Median | Mean | Max |
| (01) Nano-Rev (<\$50M) | 85 | 290 | 49,000 | 215,297 | 7,130,000 |
| (02) Micro-Rev (\$50M-\$300M) | 44 | 1,000 | 88,154 | 487,411 | 6,570,000 |
| (04) Small-Rev (\$300M-\$2B) | 23 | 4,178 | 118,671 | 599,907 | 5,650,000 |
| (05) Mid-Rev (\$2B-\$10B) | 9 | 2,662 | 91,457 | 173,851 | 678,000 |
| (07) Large-Rev (\$10B-\$100B) | 8 | 1,603,800 | 3,326,313 | 5,965,571 | 15,000,000 |
| (08) Mega-Rev (> \$100B) | 1 | 11,491,000 | 11,491,000 | 11,491,000 | 11,491,000 |
| (99) Unknown | 2 | 7,338 | 9,482 | 9,482 | 11,625 |
| | 172 | | | | |

- (08) Mega-Rev (> \$100B)
- (99) Unknown

Security Statistics

Quick Hits

Compiled from:
- NetDiligence/RSM Annual Cyber Claims Study

The average per-record cost was \$17K. The median per-record cost was \$39.82. This extraordinarily high per record average has been driven by three large outliers: fewer than 10 records each, with per record costs between \$35K and \$1.6M.

PII was the most frequently exposed data (40% of claims), followed by PCI (27%) and PHI (15%).

Hackers were the most frequent cause of loss (23%), followed by Malware/Virus (21%). Following at third and fourth were Staff mistakes (9%) and Rogue employees (7%).

Healthcare was the sector most frequently breached (19%), followed by Professional Services (13%).¹

The average cost for Crisis Services (forensics, notification, credit monitoring, legal guidance/Breach Coach® and miscellaneous other response costs) was \$357K. The median cost for Crisis Services was \$43K.

The average cost for legal defense was \$130K. The median cost for legal defense was \$16K.

Security Statistics

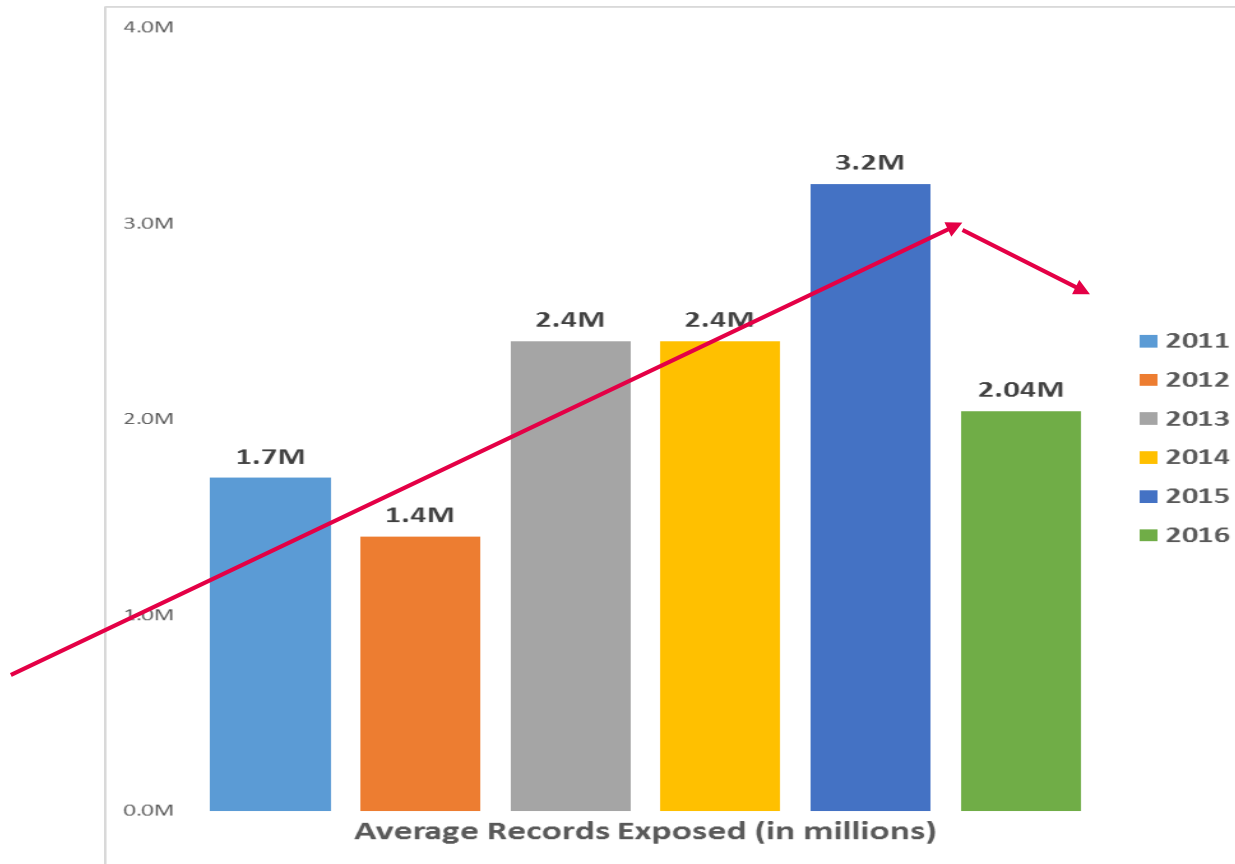
Quick Hits

Compiled from:
- NetDiligence/RSM Annual Cyber Claims Study

- Third parties accounted for 13% of the claims.
- There was insider involvement in 30% of the claims.
 - This includes mistakes and errors (77% were unintentional)
 - Also includes rogue employees and purposeful malicious actions
- The average cost for legal settlement was \$815k.
- 75% of costs were tied to Crisis Services
 - Incident Response, hotlines, notifications, etc.
 - The costs were compounded by the organizations not having robust incident response plans
- Ransomware average costs were \$32k but raising quickly
- The average claim payout was \$495K.

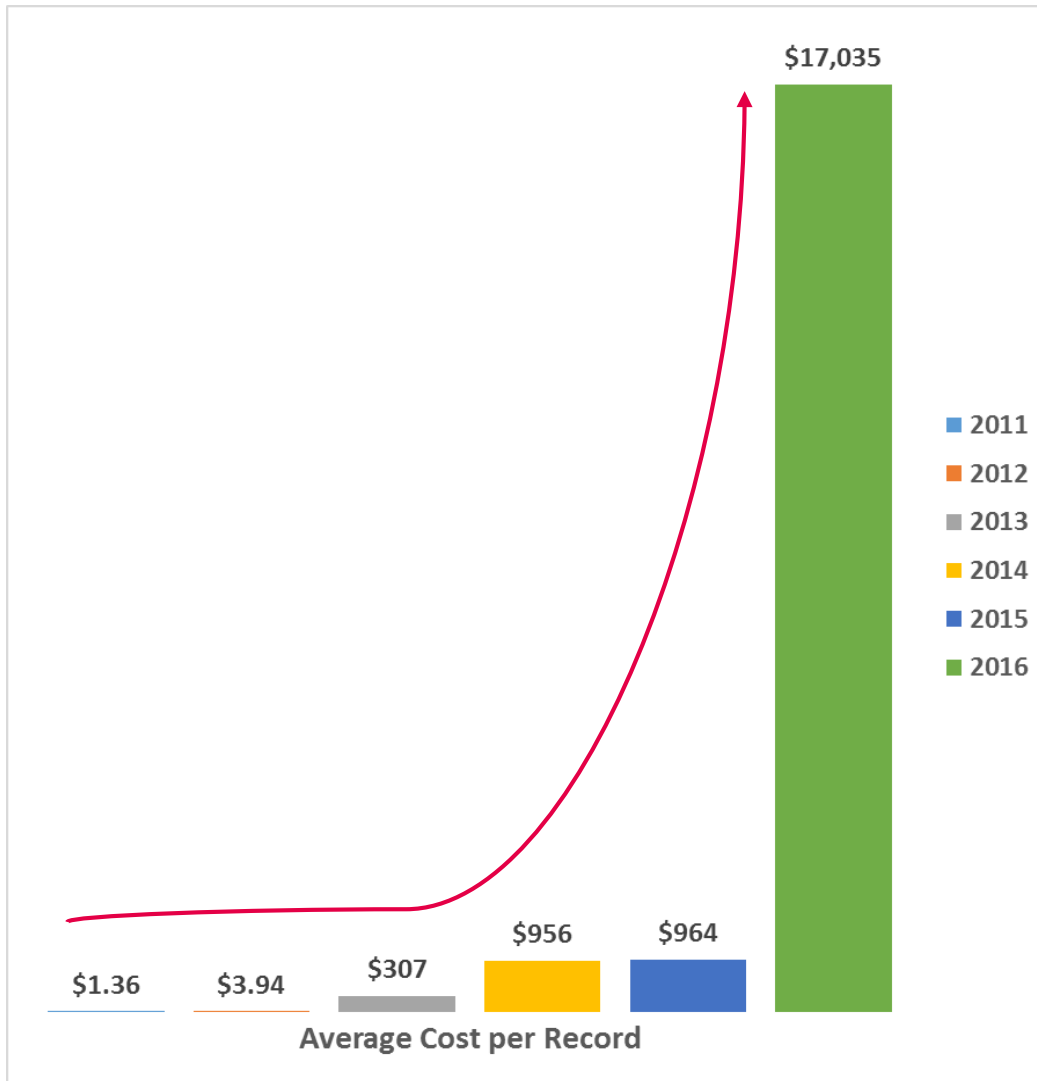
Security Statistics

Compiled from:
- NetDiligence/RSM Annual Cyber Claims Study



Security Statistics

Compiled from:
- NetDiligence/RSM Annual Cyber Claims Study



The linkage has broken between the cost of a breach being tied to the number of records that were exposed.

THREAT OVERVIEW



Threat Overview

Most Common Current Risks

| | |
|----------------------------|--|
| 1. Loss of IP | <ul style="list-style-type: none">• Blueprints, formulas, production methods, R and D, pricing sheets• Often extremely hard to prove• Side note: What if data is manipulated in addition to being taken? |
| 2. Business Interruption | <ul style="list-style-type: none">• Interruption of manufacturing, shipping, etc.• Violation of contracts, loss of revenue, reputational damage, etc. |
| 3. Bank Account Compromise | <ul style="list-style-type: none">• Business plan: Find the person that can move money. Take over their computer. Profit.• Alternative: Find the person that can move money. Ask them to give me money. Profit. |
| 4. Loss of Sensitive Data | <ul style="list-style-type: none">• Mid-Market is not know for mass quantities of PII, but they often have enough to count (i.e. hurt)• Relatively immature controls (as compared to other industries) makes even small loses of PII problematic for fines/lawsuits |

Threat Overview

Common Current Threats

| | |
|--|---|
| 1. Social Engineering  | <ul style="list-style-type: none">• Why bother to do all the heavy lifting involved with “hacking” when you can just ask someone to do something for you?• While there is a technical component the attack is against human nature |
| 2. Malware  | <ul style="list-style-type: none">• Finding and purchasing non-detectable malware in the underground market is trivial• Current focus on ransomware |
| 3. Hacking | <ul style="list-style-type: none">• “Traditional” hacking is used post-breach not as the original entry point• Current methods focus on web apps and browser plug-ins |
| 4. Physical Loss | <ul style="list-style-type: none">• Rare occurrence but significant impact |

Threat Overview

Social Engineering

- Rise of the “low tech” hack
- Very polished method of social engineering that does not require actual “hacking”
- Fancy name for traditional “con games”
 - Attacking an environment via manipulating people
- Hacking by the KISS principle
 - Keep it simple, stupid
- Why go through all of the effort to bypass firewalls, anti-virus, monitoring solutions, etc.?
- Why not just have the target do all the work for you?



Threat Overview

- Vendor Fraud aka. Invoice Fraud aka. Supply Chain Fraud:
 - Attacker identifies a vendor of the organization
 - Attacker attempts to convince the organization to make a normal or additional payment to a new account
 - Organization unaware of fraud until notified by the vendor
 - Typical example:

To: [Someone in finance]
From: Executive@vend0r.com
Sent: Mon, Oct 5, 2015 at 2:01am

Mr/Mrs. Someone, please be aware that we have recently changed banking providers. Our new account and routing numbers are in the attached pdf.
Respectfully, Mr. Vendor Executive

Threat Overview

- Fake Executives:
 - Often create entire fake email chains including supposed communications with other executives
 - May tie to fake vendor claims, but also tax payments, legal fines, issuing corporate credit cards, fake checks, etc.
 - Utilizes organizational and positional pressure to succeed
 - Typical Example:

To: [Someone in finance]
From: Executive@ourc0mpany.com
Sent: Mon, Oct 5, 2015 at 2:01am

Hey, [nickname]. I was just contacted by one of our key vendors and it looks like we missed a payment last month. We are currently negotiating next year's contract so this is VERY sensitive. Immediately wire \$xxx,xxx to the attached account information or there will be hell to pay for all of us.

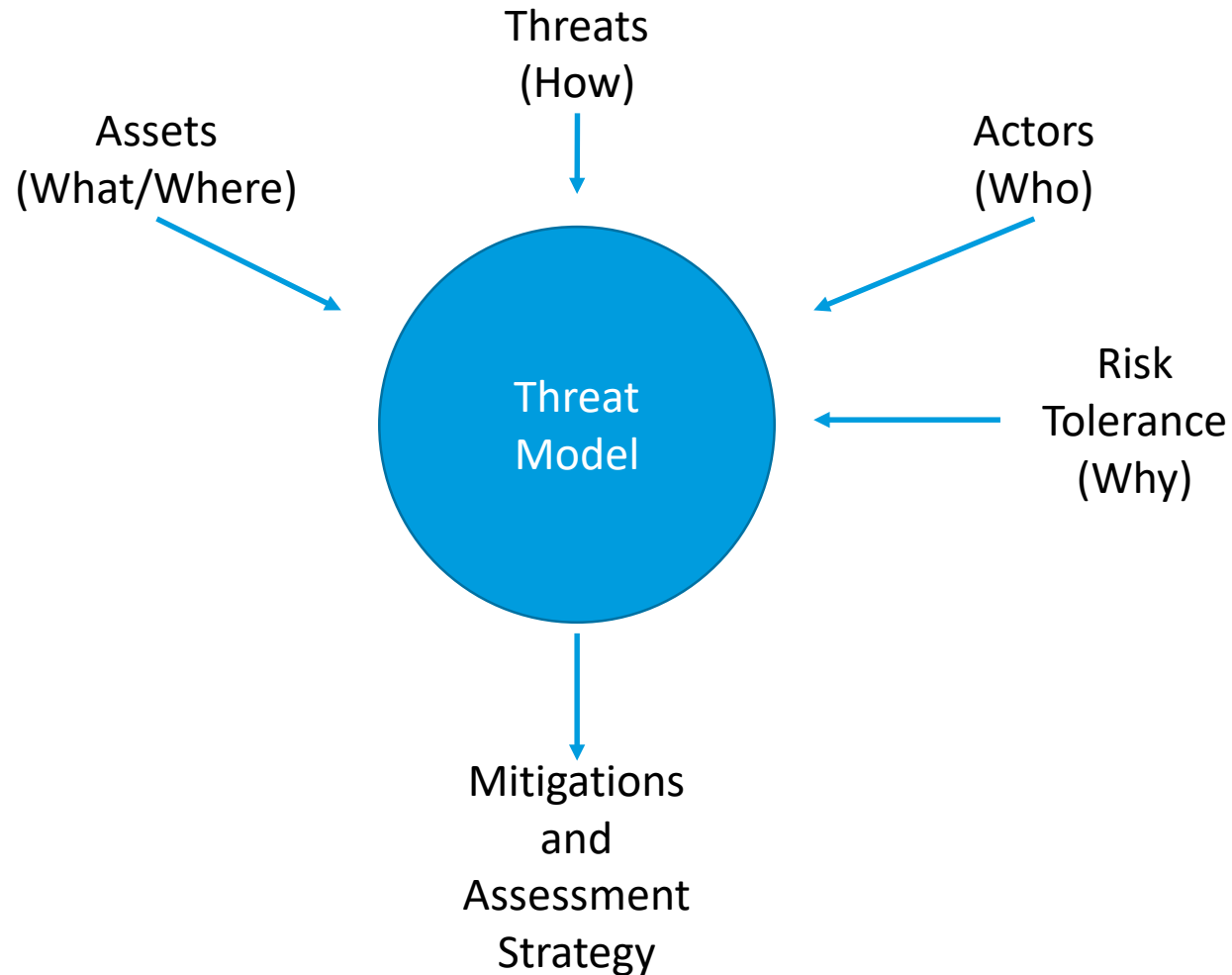
Respectfully, CEO Executive

Threat Overview

- Malicious Emails
 - Malicious attachment that directly installs the ransomware
 - Link to malicious websites that will ultimately lead to the malware being installed on the system
- Exploit Kits
 - Poisoned Documents
 - Malvertisements
 - Redirected web traffic from traffic distribution services.
- Manual: Brute forcing password to remote access and/or deployed as part of a traditional environmental compromise
- Exploit server vulnerabilities
- Starting to add other functionality: Credential harvesting, poison backups, etc.

RECOMMENDATIONS

Threat Modeling Methodology



Actors (Who)

Who are the bad actors you're concerned with?

- Employee
- Contractor
- Customer
- Random attacker
- Focused attacker
- State-sponsored attacker



Actors
(Who)



Threats (How)

How are the bad actors going to attack you?

- From the Internet
- From your internal network
- From your wireless network
- Via Email
- From USB keys
- From the phone

Threats
(How)



Assets (What/Where)

What data do they want?

- Customer records
- Employee records
- Money transfer
- Money laundering
- Ransomware

What data elements are they trying to steal?

- Social Security numbers
- Credit card
- W2
- ACH/account number

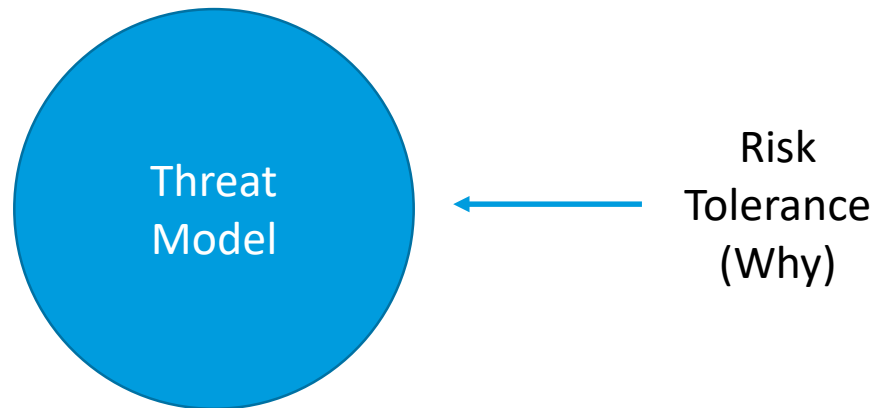
Assets
(What/Where)



Risk Tolerance (Why)

Every “scenario” has a cost.
What is your risk tolerance?

- Financial risk
- Brand risk
- Operational risk

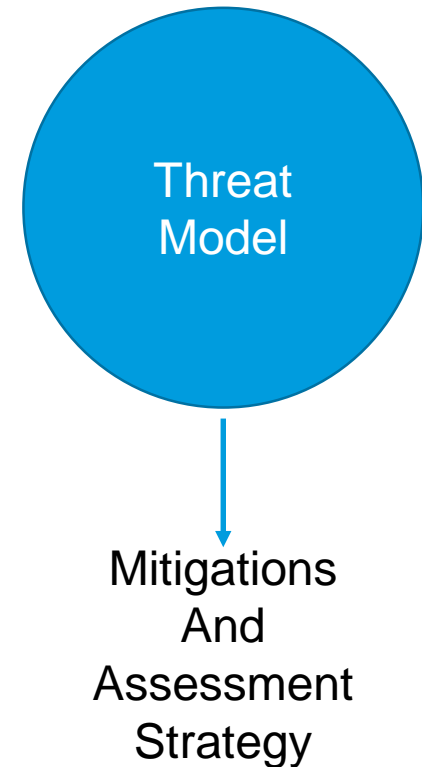


Mitigations

The result is a set of scenarios that are most important to you.

You use these scenarios to:

- Assess the likeliness of being impacted from them
- Build a strategy to protect yourself against them
- Hedge your losses against them with cyberinsurance
- Accept the risk



Example Threats

The following are example threats to consider:

- An attacker getting an employee to execute something to get on your network
- Random attacker gaining access to your network and stealing data
- Focused attacker gaining access to your critical data and servers
- Customer gaining inappropriate access to other customers data



Recommendations

- Payment controls
 - Offline vendor contact lists
 - Multiple approvals
 - Protocols for emergency payments including out-of-band communications, executive PINs/Passwords, etc.
- Account Takeovers
 - Two factor authentication
 - Multiple terminals used for multiple approvals
 - Payment limits without verbal approvals
- Ransomware
 - Backups of critical data on a frequent basis
 - Arranged DDoS protection with vendor and ISP
 - Pre-determined course of action for payment or non-payment

Recommendations

- What is your decision making process on ransomware?
- What do you take into account?
 - What is the importance of the systems?
 - Is it likely to have sensitive data?
 - Are you likely to have backups?
 - Is it worth the cost to decrypt?
 - Is any type of investigation necessary?
 - If so, what would you recommend?
 - If so, how would you do it?

Recommendations

- Network Management
 - Network segmentation
 - Why have critical systems on the same network as users?
 - Why have sensitive data sources in the same situation?
 - Security monitoring
 - Network level anti-virus
 - User activity
- Data Management
 - What do you have?
 - Where is it?
 - Who has access to it?
 - Why?
 - Can it be reduced?

Recommendations

- Insurance: Cover all sources of loss
 - Calculate potential losses
 - Business interruptions
 - Contract violations
 - Value of IP
 - [Amount of PII] X [average cost per record]
 - Consultants, forensics, lawyers, recovery costs/manhours
- Insurance: Cover all the event types
 - Malware
 - Ransom
 - Social Engineering
 - Employee mistake
 - Etc.



QUESTIONS AND ANSWERS?