SBS INSTITUTE

VBA Connect & Protect Experience: What to Do When Your Vendor Gets Hacked

Presented By: Terry Kuxhaus CISSP
Senior IS Consultant/Regional Director - SBS CyberSecurity, LLC

Contact Information

SBS CyberSecurity

Follow us on Social:

Terry Kuxhaus (CISSP)

- Senior IS Consultant/Regional Director
- Bachelors of Science in Technology for Black Hills State University
- Terry.kuxhaus@sbscyber.com
- 605-222-7400
- www.sbscyber.com

SBS Institute

- sbsinstitute@sbscyber.com
- 605-269-0909

Session Agenda

- Types of Vendor Breaches
- Examples of Vendor Breaches
- Key Components of modern Vendor Management
- Vendor Management + Incident Response
- Controls to Reduce Vendor Breach Risk
- Digital Forensics’ role
- Insurance and Legal

SBS INSTITUTE

Types of Vendor Breaches

“Vendor Breach” is not a single situation; what are the different types?

4 Common Types of Vendor Breaches

- **Hacking**
  - Intentional access or harm to data/assets by circumventing security or exploiting vulnerabilities
  - Denial of Service/DDoS – Create Diversion
- **Account Takeover/BEC**
  - Stolen/Compromised Credentials
- **Social Engineering/Phishing – involved in 82% of all breaches**
  - Vendors are becoming huge target
- **Malware/Malicious**
  - Ransomware, Trojans, Spyware
- **Error/Misconfiguration**
  - Security settings not properly implemented
  - Unpatched or unsupported systems

What access does your Vendor have?

- **Direct access to your network**
  - **Target**
- **Cloud hosting**
  - Hosting your network
  - Hosting network devices, including servers
  - Hosting email
  - Hosting data
- **Data Center hosting**
  - you have access to a system via VPN/direct connection

What access does your Vendor have?

- **SaaS apps** – apps you access via the internet
- **Direct access to apps on your network**
  - **SolarWinds**
- **Vendor stores data about you or your customers**
  - **Core Banking**
  - **Equifax**
- **Vendor processes transactions for you or your customers**
  - Card processors
- **Vendor email compromise**

SBS INSTITUTE

Examples of Vendor Breaches

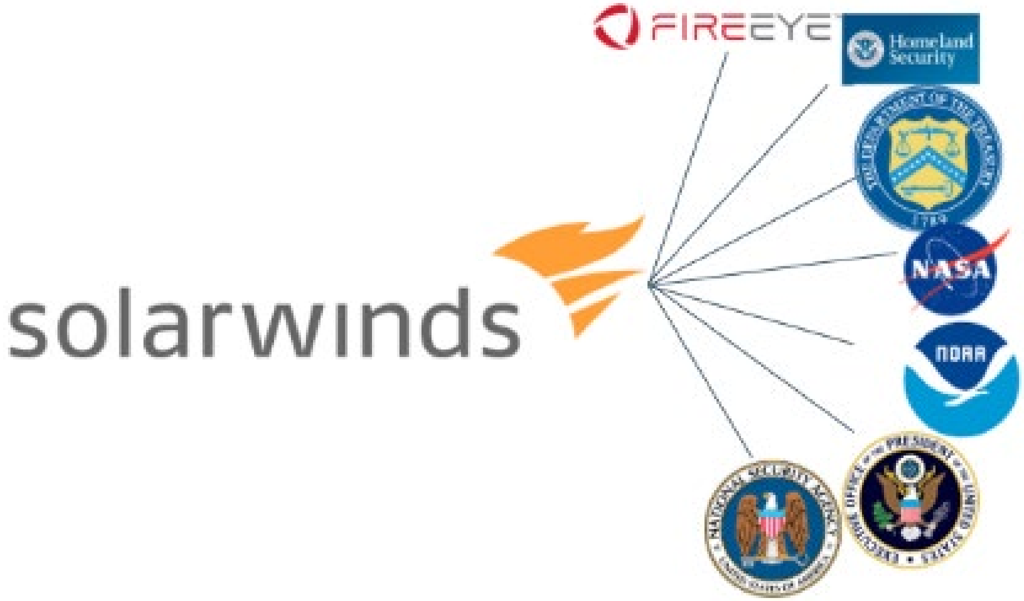
What are some of the most impactful Vendor Breaches?

Flagstar Bank (2022 and 2021)

- 2021 – Third Party (Accellion) File Sharing platform used by Flagstar hit with Ransomware.
  - Many orgs affected - Kroger, Law Firms, Shell, etc
  - Names, SSNs, addresses stolen
- 2022: 1.5 million customer records stolen from corporate network
  - Names, SSNs, addresses stolen
  - Took 6 months for Flagstar to report
  - **Drove the 36-hour notification rule for FDIC and OCC orgs**

SolarWinds (2020)

- SolarWinds network compromised in 2019
- Orion product code accessed by attackers, and malicious code injected
- Updates pushed out to customers
- Backdoor access into customer networks established (18,000 orgs)
- Access to customer networks and data exfiltration



American Bank Systems (2020)

- Document management and compliance provider for banks
- Hit with Avaddon ransomware and network compromise
- Avaddon hit over 50GB of data, including:
  - Loan documents
  - Contracts
  - Private emails
  - Invoices
  - Credentials for network shares
  - Confidential company files

American Bank Systems
The compliance company for the banking industry

MSPs hit with Ransomware (2019)

- One MSP in Texas – **TSM Consulting** - hosted services for 22 local community governments and 300 law enforcement agencies in TX suffered a ransomware attack
  - Fortunately, 96% of systems were restored within 48 hours, according to the company
  - Data exfiltration was not determined
- **CyrusOne** – a large global data center – also suffered a ransomware attack, crippling numerous customers from its NY data center
- MSPs are an easy lever for attackers to pull and affect numerous clients at one time

LastPass (2022) x2

- **August:** LastPass discloses that an "unauthorized party" gained access to a "third-party cloud-based storage service" used by LastPass to store archived production backups. "No customer or vault data was taken," but some source code and technical information was stolen.
- **December:** LastPass discloses another incident has occurred as a result of the August 2022 incident. The threat actor targeted a senior DevOps engineer using information obtained during the August 2022 incident. The threat actor was able to exploit "vulnerable third-party software" to deliver malware, bypass controls, and gain unauthorized access to cloud backups.

https://blog.lastpass.com/2022/12/notice-of-recent-security-incident

LastPass Recommended Actions

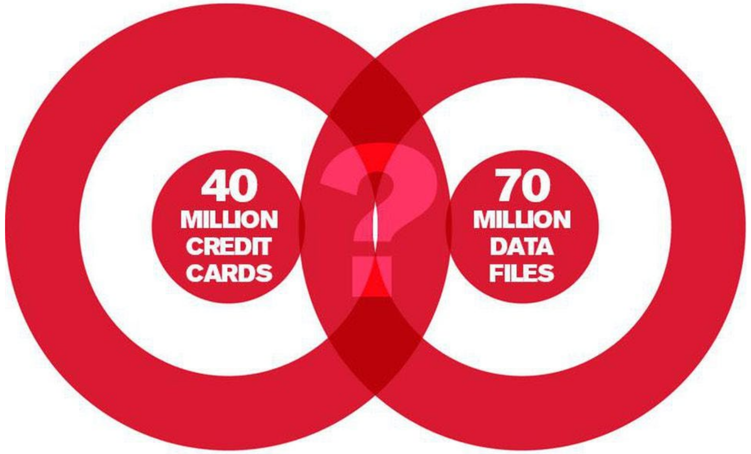
- Make sure strong and unique master passwords of least 12 characters long (ideally 16-20 characters) are required. Computer-generated random passwords are best. Also, enable the following features (controls):
  - Require master password change when reuse detected
  - Prohibit reuse of old master passwords
  - Minimum character sets in master password (at least 2; preferably 3)
- Review security reports related to master passwords; look for:
  - Reused master password
  - Weak master password
  - Reset select master passwords (optional)
- Review and increase master password iteration count settings – in January 2023, OWASP updated the recommended number of PBKDF2 iterations to 600,000.
- Review shared folders accessed by users with a low iteration count
- Ensure super admins follow master password and iterations best practices

LastPass Recommended Actions

- Ensure super admins follow master password and iterations best practices
- Review super admins with “Permit super admins to reset master passwords” policy rights and weak master passwords/iterations
- Review super admins with "Permit super admins to access shared folders" rights
- Require MFA and reset shared secrets (for non-federated customers)
- Exposure due to unencrypted data - generate URL reports to assess risk
- Reset SCIM, Enterprise API, and SAML Keys
- Review user security scores and remediate as required
    - SBS recommends changing the passwords to any critical application (email, financial/banking, business apps, etc.) as well, just to be safe.
- Turn on dark web monitoring for users
- Review security of shared folders

https://support.lastpass.com/help/security-bulletin-recommended-actions-for-business-administrators

The infamous others



HOME
DEPOT
HACKED
56 MILLION CUSTOMER
CREDIT & DEBIT CARD
DATA EXPOSED

DATA
BREACH
Marriott
INTERNATIONAL
starwood
Hotels and
Resorts

SBS INSTITUTE

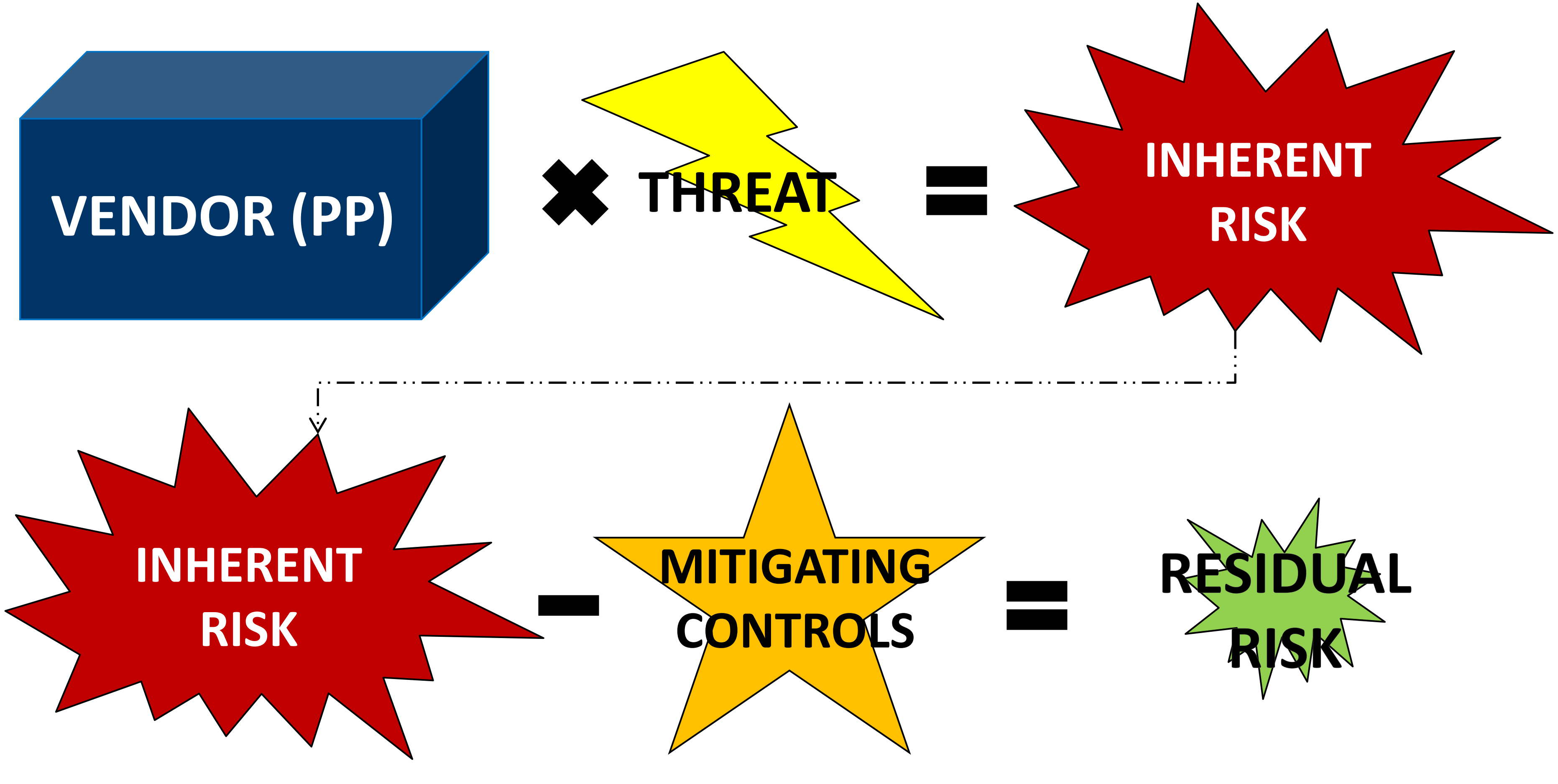
Modern Vendor Management Components

What should you be doing to manage vendor risk today?

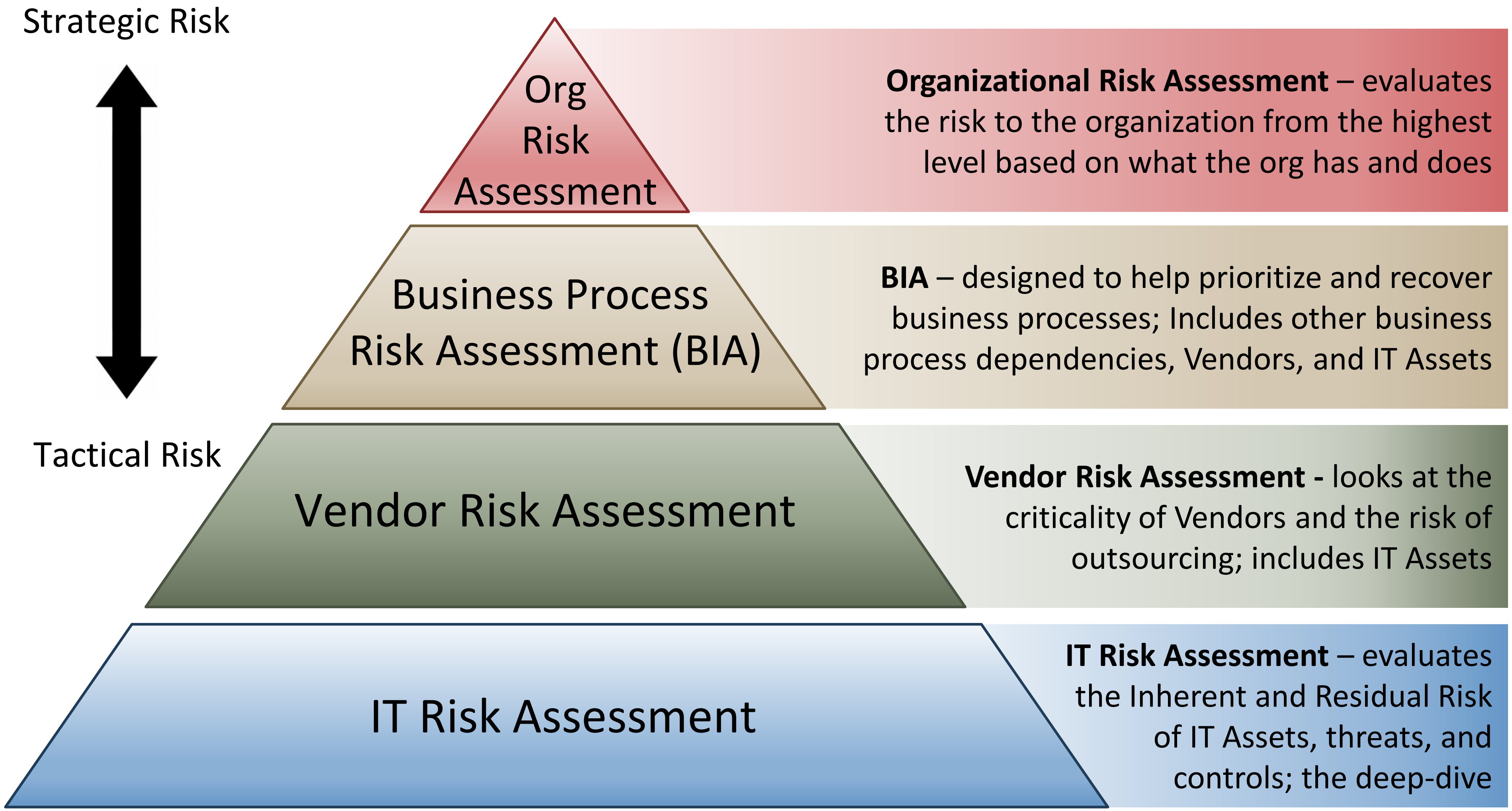
Vendor Risk Assessment

- All of your risk assessments should help you to make DECISIONS.
- What are the decisions we want to make out of our Vendor Risk Assessment?
  - **Who to do business with? (Vendor Selection)**
  - **Do I want to continue to do business with this vendor? (Ongoing Vendor Management)**
- How do you build a quantifiable and measurable Vendor Risk Assessment?

Vendor Risk Assessment Components



Risk Management Hierarchy



Organizational Risk Assessment – evaluates the risk to the organization from the highest level based on what the org has and does

BIA – designed to help prioritize and recover business processes; Includes other business process dependencies, Vendors, and IT Assets

Vendor Risk Assessment - looks at the criticality of Vendors and the risk of outsourcing; includes IT Assets

IT Risk Assessment – evaluates the Inherent and Residual Risk of IT Assets, threats, and controls; the deep-dive

Vendor Risk Assessment

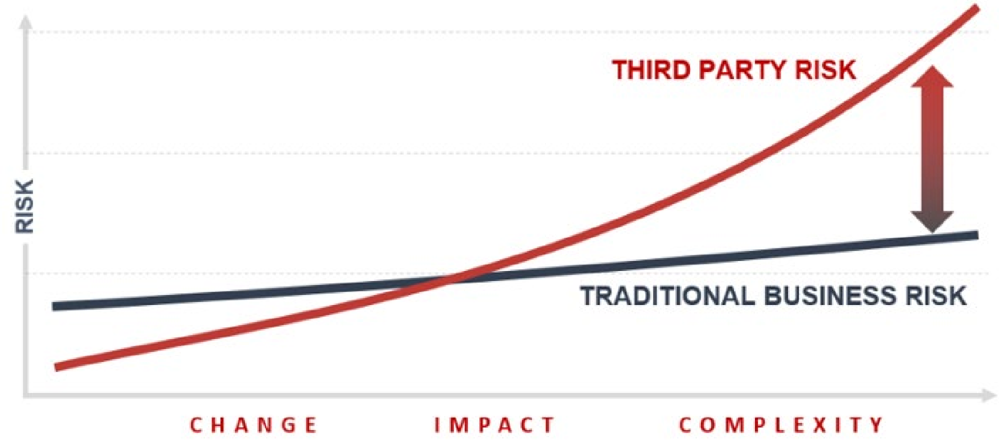
- Start with the "**Protection Profile**"
  - How important is this vendor?
  - Areas of measurement:
    1. **Store, Transmit, or Process** confidential customer info?
    2. **Access** to your customer info?
    3. How critical is it that this vendor be **Available** to us?
    4. How many **IT Assets** (or systems/apps) to they provide to us?

IMPORTANT!

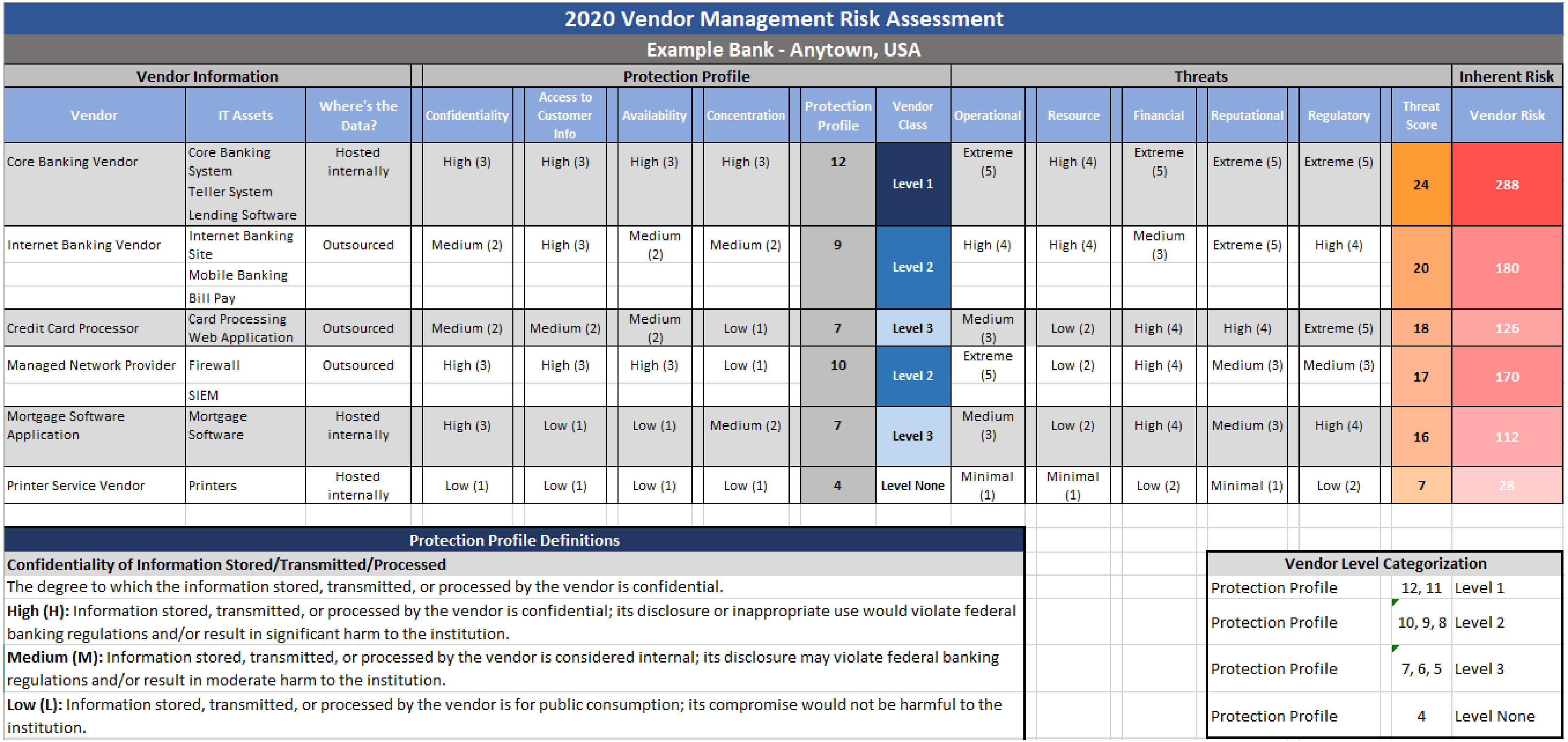
Vendor Risk Assessment

- Determine **Threats**:
  - OCC and FFIEC list out five (5) categories of risk:
    1. Operation
    2. Compliance
    3. Strategic
    4. Reputation
    5. Credit

Digital Transformation introduces
Third Party Risk



Vendor Risk Assessment



2020 Vendor Management Risk Assessment

Example Bank - Anytown, USA

Vendor Information			Protection Profile						Threats						Inherent Risk
Vendor	IT Assets	Where's the Data?	Confidentiality	Access to Customer Info	Availability	Concentration	Protection Profile	Vendor Class	Operational	Resource	Financial	Reputational	Regulatory	Threat Score	Vendor Risk
Core Banking Vendor	Core Banking System Teller System Lending Software	Hosted internally	High (3)	High (3)	High (3)	High (3)	12	Level 1	Extreme (5)	High (4)	Extreme (5)	Extreme (5)	Extreme (5)	24	288
Internet Banking Vendor	Internet Banking Site Mobile Banking Bill Pay	Outsourced	Medium (2)	High (3)	Medium (2)	Medium (2)	9	Level 2	High (4)	High (4)	Medium (3)	Extreme (5)	High (4)	20	180
Credit Card Processor	Card Processing Web Application	Outsourced	Medium (2)	Medium (2)	Medium (2)	Low (1)	7	Level 3	Medium (3)	Low (2)	High (4)	High (4)	Extreme (5)	18	126
Managed Network Provider	Firewall SIEM	Outsourced	High (3)	High (3)	High (3)	Low (1)	10	Level 2	Extreme (5)	Low (2)	High (4)	Medium (3)	Medium (3)	17	170
Mortgage Software Application	Mortgage Software	Hosted internally	High (3)	Low (1)	Low (1)	Medium (2)	7	Level 3	Medium (3)	Low (2)	High (4)	Medium (3)	High (4)	16	112
Printer Service Vendor	Printers	Hosted internally	Low (1)	Low (1)	Low (1)	Low (1)	4	Level None	Minimal (1)	Minimal (1)	Low (2)	Minimal (1)	Low (2)	7	28

Protection Profile Definitions

Confidentiality of Information Stored/Transmitted/Processed

The degree to which the information stored, transmitted, or processed by the vendor is confidential.

High (H): Information stored, transmitted, or processed by the vendor is confidential; its disclosure or inappropriate use would violate federal banking regulations and/or result in significant harm to the institution.

Medium (M): Information stored, transmitted, or processed by the vendor is considered internal; its disclosure may violate federal banking regulations and/or result in moderate harm to the institution.

Low (L): Information stored, transmitted, or processed by the vendor is for public consumption; its compromise would not be harmful to the institution.

Vendor Level Categorization		
Protection Profile	12, 11	Level 1
Protection Profile	10, 9, 8	Level 2
Protection Profile	7, 6, 5	Level 3
Protection Profile	4	Level None

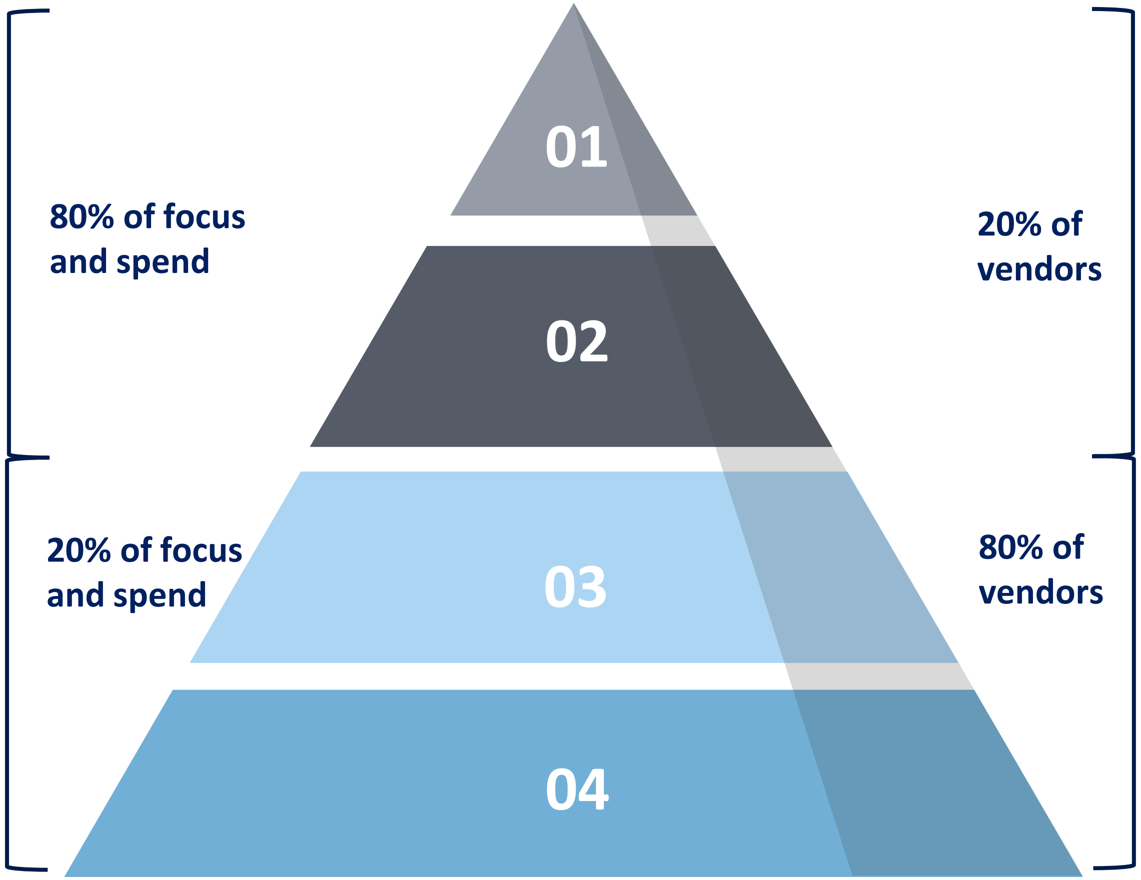
Vendor Levels

01 INSTITUTION-WIDE CRITICAL VENDORS

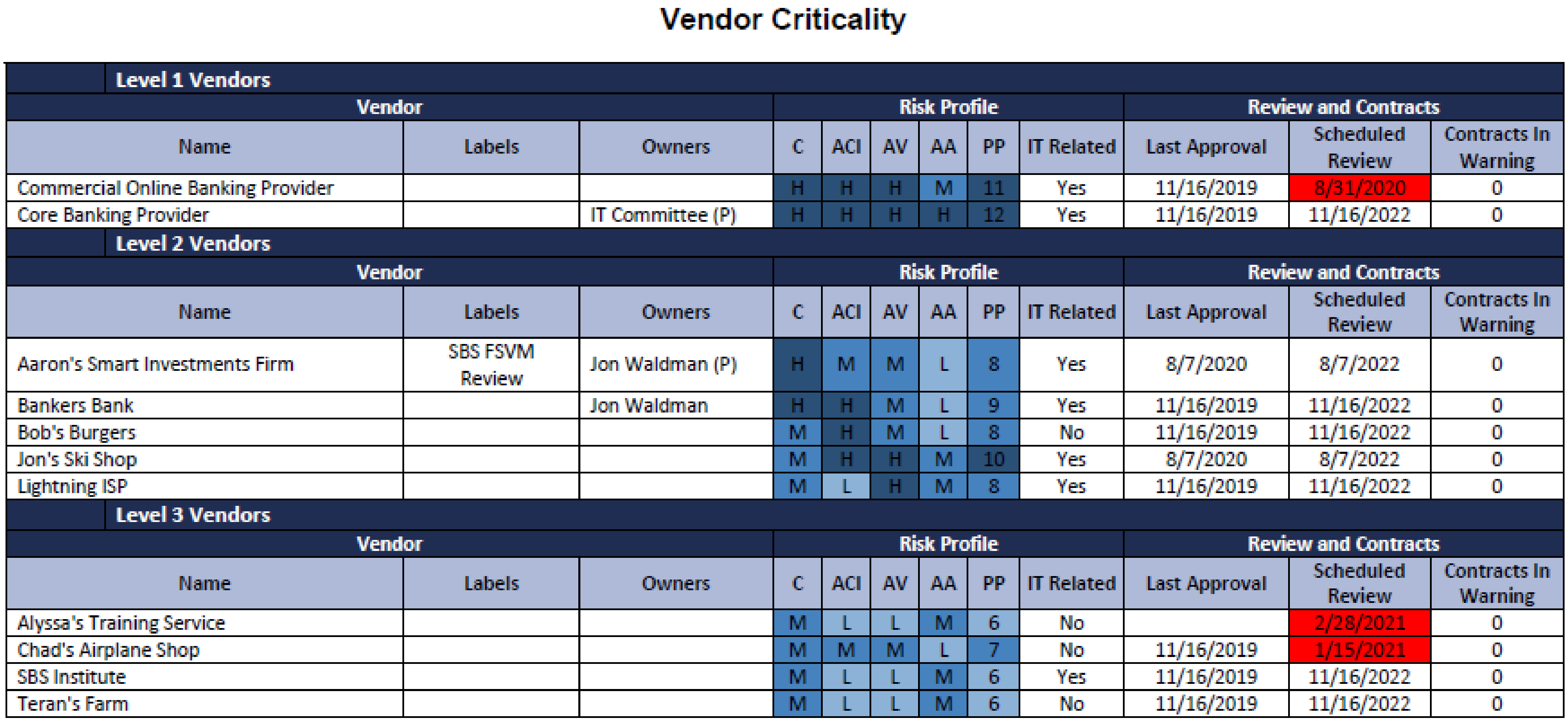
02 SIGNIFICANT VENDORS

03 NON-ESSENTIAL VENDORS

04 EXEMPT VENDORS



Example of Vendor Levels



Vendor Criticality

Level 1 Vendors

Vendor			Risk Profile						Review and Contracts		
Name	Labels	Owners	C	ACI	AV	AA	PP	IT Related	Last Approval	Scheduled Review	Contracts In Warning
Commercial Online Banking Provider			H	H	H	M	11	Yes	11/16/2019	8/31/2020	0
Core Banking Provider		IT Committee (P)	H	H	H	H	12	Yes	11/16/2019	11/16/2022	0

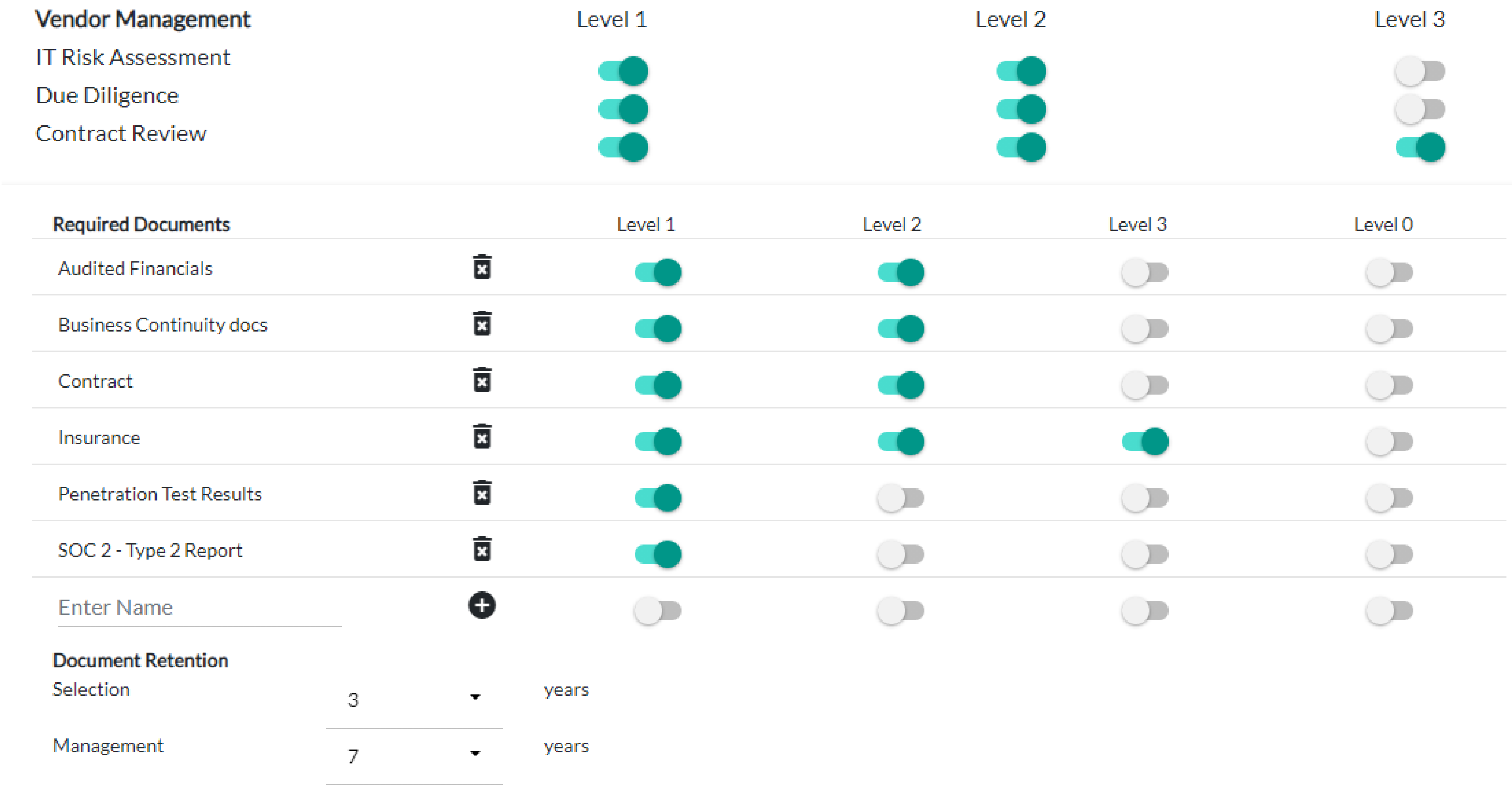
Level 2 Vendors

Vendor			Risk Profile						Review and Contracts		
Name	Labels	Owners	C	ACI	AV	AA	PP	IT Related	Last Approval	Scheduled Review	Contracts In Warning
Aaron's Smart Investments Firm	SBS FSVM Review	Jon Waldman (P)	H	M	M	L	8	Yes	8/7/2020	8/7/2022	0
Bankers Bank		Jon Waldman	H	H	M	L	9	Yes	11/16/2019	11/16/2022	0
Bob's Burgers			M	H	M	L	8	No	11/16/2019	11/16/2022	0
Jon's Ski Shop			M	H	H	M	10	Yes	8/7/2020	8/7/2022	0
Lightning ISP			M	L	H	M	8	Yes	11/16/2019	11/16/2022	0

Level 3 Vendors

Vendor			Risk Profile						Review and Contracts		
Name	Labels	Owners	C	ACI	AV	AA	PP	IT Related	Last Approval	Scheduled Review	Contracts In Warning
Alyssa's Training Service			M	L	L	M	6	No		2/28/2021	0
Chad's Airplane Shop			M	M	M	L	7	No	11/16/2019	1/15/2021	0
SBS Institute			M	L	L	M	6	Yes	11/16/2019	11/16/2022	0
Teran's Farm			M	L	L	M	6	No	11/16/2019	11/16/2022	0

Vendor Management Requirements



Vendor Management	Level 1	Level 2	Level 3
IT Risk Assessment	●	●	○
Due Diligence	●	●	○
Contract Review	●	●	●

Required Documents		Level 1	Level 2	Level 3	Level 0
Audited Financials	🗑	●	●	○	○
Business Continuity docs	🗑	●	●	○	○
Contract	🗑	●	●	○	○
Insurance	🗑	●	●	●	○
Penetration Test Results	🗑	●	○	○	○
SOC 2 - Type 2 Report	🗑	●	○	○	○
Enter Name	⊕	○	○	○	○

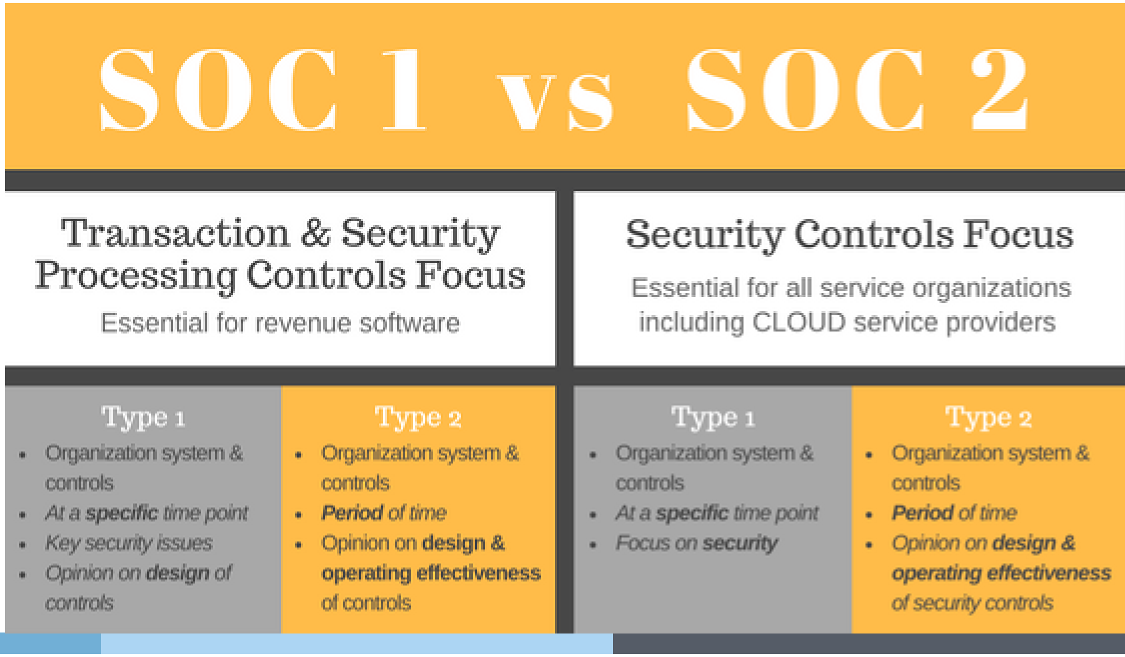
Document Retention

Selection	3 ▾	years
Management	7 ▾	years

Models to Manage Vendor Risk

SBS INSTITUTE

- The goal: understand how the Vendor protects your data:
  - Documentation from vendors (SSAE-18, SOC, or other audit reports)
  - BITS Shared Assessments/VRMMM
  - ISO 27002 Gap Assessment
  - PCI Self Assessment (vendor)
  - On-site visits to vendors
  - Tools (TRAC)
  - Your own Questionnaires



SOC 1 vs SOC 2

Transaction & Security Processing Controls Focus		Security Controls Focus	
Essential for revenue software		Essential for all service organizations including CLOUD service providers	
Type 1	Type 2	Type 1	Type 2
• Organization system & controls • *At a **specific** time point* • *Key security issues* • *Opinion on **design** of controls*	• Organization system & controls • ***Period** of time* • Opinion on **design & operating effectiveness** of controls	• Organization system & controls • *At a **specific** time point* • *Focus on **security***	• Organization system & controls • ***Period** of time* • *Opinion on **design & operating effectiveness** of security controls*

Due Diligence & Contract Review

- Stare with Regulatory guidance: FFIEC, FRB, FDIC, & OCC
- However, you should look into some other questions to ask, rather than just focusing FDIC & OCC questions, such as:
  - **SOC Review Questions** – what is important to take away from a SOC review?
  - **Cloud Computing Questions**
  - **Foreign-Based Service Provider Questions**
- Just as different documentation requirements should be set for different levels of vendor, so should the amount and types of questions.
- **The more critical the vendor, the deeper the dive into Contract Review and Due Diligence questions**

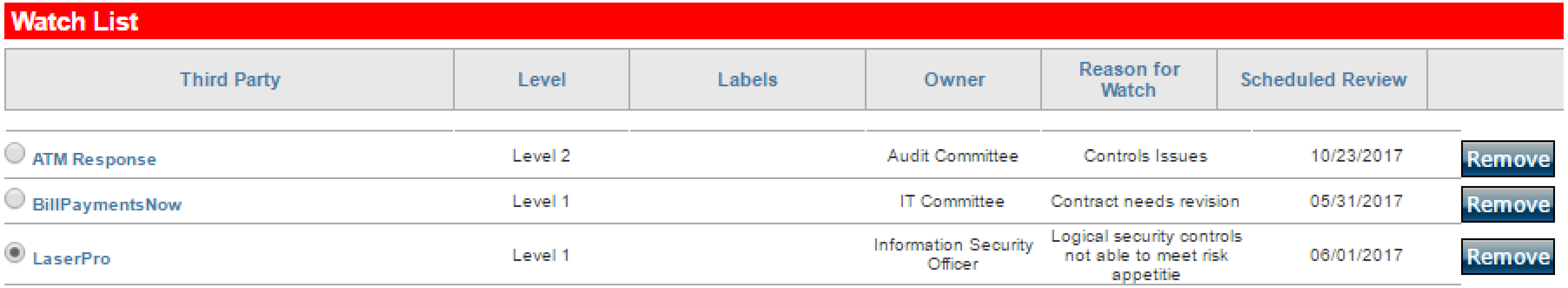
The Watch List

- When a vendor does not meet acceptable levels of risk (does not “pass” a vendor review), the vendor should be placed on a Watch List
- The Watch List has four (4) outcomes:
  1. **Accept the Risk**
  2. **Resolve the Risk**
     - Work with the vendor to address any issues until resolved, then remove the vendor from the Watch List
  3. **Change the Risk**
     1. Find a new vendor
     2. Bring the product in-house (if outsourced) for more control
     3. Discontinue the product or service
  4. **Transfer the Risk**

AVOID
ACCEPT
RISK
MANAGEMENT
REDUCE
TRANSFER

The Watch List

- The Watch List is intended to understand who your riskiest vendors are and track that risk more frequently.



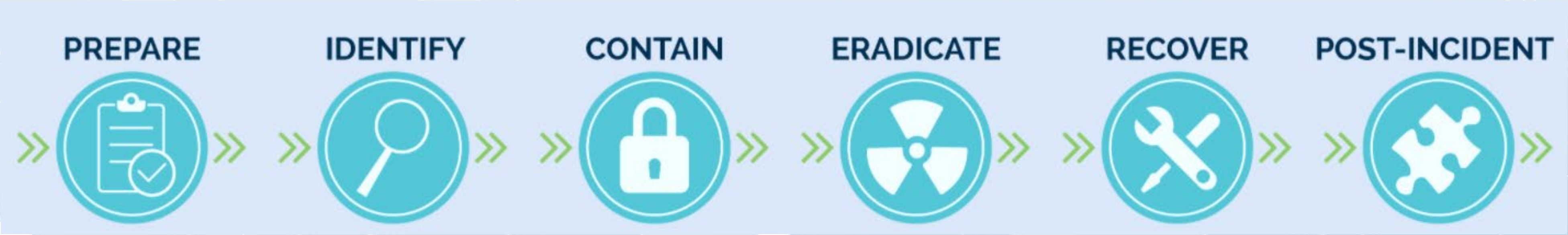
Watch List

Third Party	Level	Labels	Owner	Reason for Watch	Scheduled Review	
○ ATM Response	Level 2		Audit Committee	Controls Issues	10/23/2017	Remove
○ BillPaymentsNow	Level 1		IT Committee	Contract needs revision	05/31/2017	Remove
● LaserPro	Level 1		Information Security Officer	Logical security controls not able to meet risk appetitie	06/01/2017	Remove

SBS INSTITUTE

Vendor Management + Incident Response

Vendor Breaches are more likely to occur than ever – how to you plan?

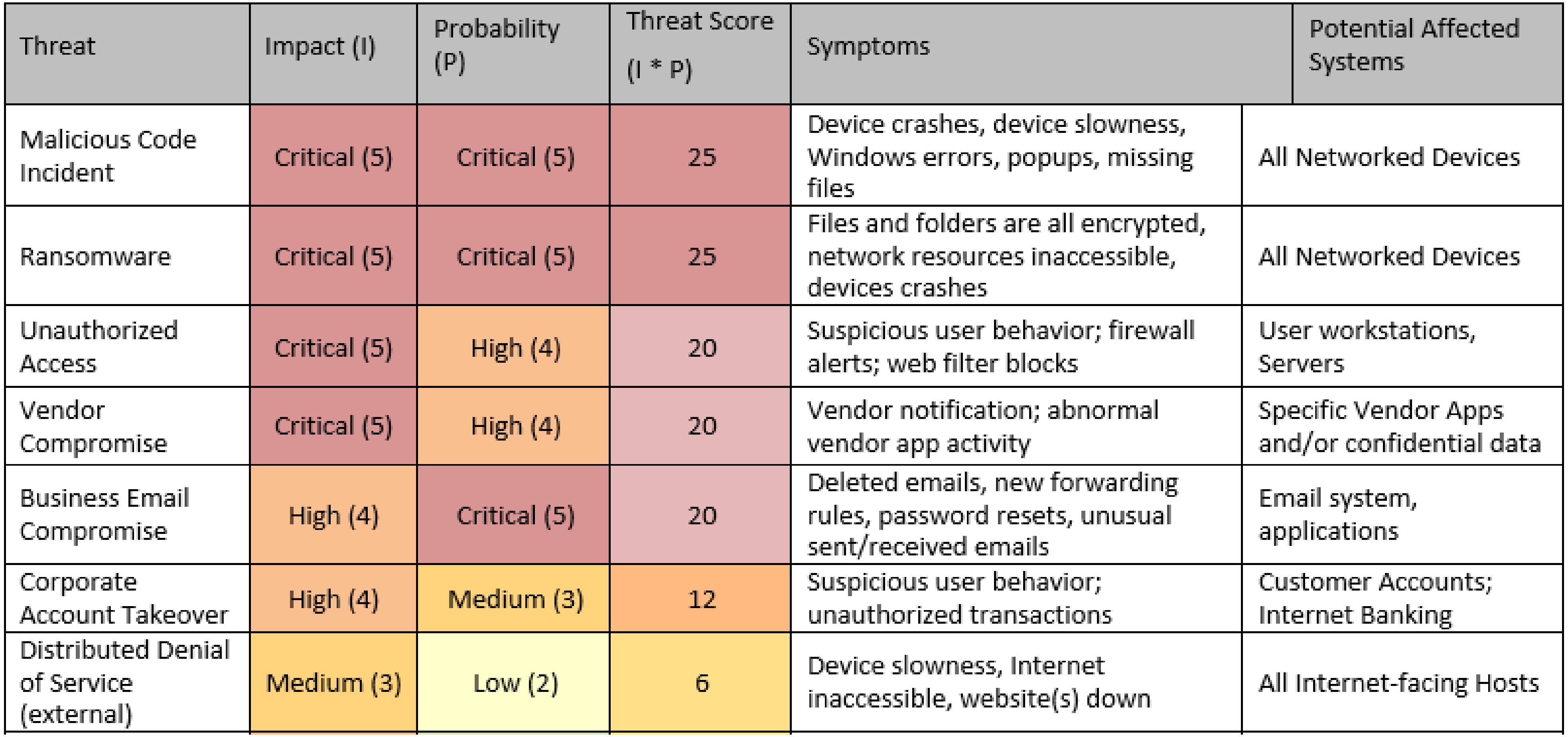


Major Questions

- The two biggest questions you can ask yourself or your vendor regarding DFIR:
  1. **If an unauthorized party was in your network, how would you know?**
  2. **If someone was sending information out the back door, would you be able to tell?**
- If you’re not certain you can answer those questions up-front, or even find the answers after the incident has occurred… please go get started **RIGHT NOW**!

Include Vendor Compromise as a Threat

- Step 1 – Know Your Threats (Incident Threat Assessment)



Threat	Impact (I)	Probability (P)	Threat Score (I * P)	Symptoms	Potential Affected Systems
Malicious Code Incident	Critical (5)	Critical (5)	25	Device crashes, device slowness, Windows errors, popups, missing files	All Networked Devices
Ransomware	Critical (5)	Critical (5)	25	Files and folders are all encrypted, network resources inaccessible, devices crashes	All Networked Devices
Unauthorized Access	Critical (5)	High (4)	20	Suspicious user behavior; firewall alerts; web filter blocks	User workstations, Servers
Vendor Compromise	Critical (5)	High (4)	20	Vendor notification; abnormal vendor app activity	Specific Vendor Apps and/or confidential data
Business Email Compromise	High (4)	Critical (5)	20	Deleted emails, new forwarding rules, password resets, unusual sent/received emails	Email system, applications
Corporate Account Takeover	High (4)	Medium (3)	12	Suspicious user behavior; unauthorized transactions	Customer Accounts; Internet Banking
Distributed Denial of Service (external)	Medium (3)	Low (2)	6	Device slowness, Internet inaccessible, website(s) down	All Internet-facing Hosts

Know which Vendors have access to what

- Review the IT Assets provided by your Vendor(s)
- Where does the IT Asset live?
- **On your network**:
  - Can the Vendor access info in or from the IT Asset?
  - Does the Vendor have direct access to your network?
- **At the Vendor:**
  - Does the Vendor have read or write access to your info?
- **In the Cloud:**
  - Does the Vendor have read or write access to your info?

Create and Modify IR Playbook Scenarios

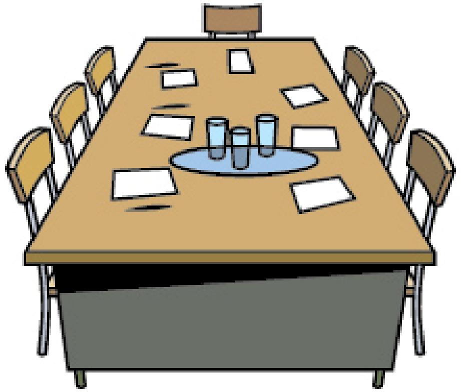
- Perform a tabletop **walkthrough** of IR scenarios on your own or with your team prior to performing an official Tabletop Test
    - For example, if your institution is concerned about a vendor breach (on the vendor's end), a part of your walkthrough scenario should discuss the types of information the vendor stores, transmits, and processes at their location on your behalf
- Update your Scenario(s) based on lessons-learned from your first-stage walkthrough.
- Keep your Scenarios up-to-date based on changes in attack tactics, vulnerabilities, or new software
- Prep your Scenarios to be as real-world as possible for the next Step

Tabletop Testing

- Take your updated Scenario(s) and perform Tabletop Testing with your Incident Response and/or Business Continuity Teams.
- Your BC/IR Teams should have a fair representation from your entire organization – not just IT/IS.
- Not only does real-world scenario Tabletop Testing with your BC/IR Teams raise awareness to how attacks really work, but also provides unique perspectives from other areas of the org you may not have considered.

Test with the Vendor + Document

- **Reach out to your Vendor** prior to the Tabletop Testing stage, and ask the vendor to participate in your Tabletop Walkthrough
- If the vendor won't/can't participate, put together a list of questions or requested information resulting from your Tabletop Test
- **Make sure to document your Tabletop Test very well as it's being performed**
  - Who attended?
  - What was the scenario?
  - What steps were determined to be taken?
  - What did you find out that you're doing well?
  - What did you find out can be improved?
  - What additional questions yet need answers?



Additional Testing

- **Comprehensive Network Security Assessments**
  - Red Team-style assessments, combining PT + VA + SE
- **Web Application Assessments**
- **Test your Web Apps (Free)**
  - Mozilla Observatory
  - Zed Attack Proxy
  - SSL labs
- **Modern Vendor Management Reviews:**
  - BitSight, Security Scorecard, FICO Cyber Risk Score
- **Ask for more testing docs during Vendor Reviews:**
  - Network Security Assessments
  - Code Reviews

Questions to Ask

The following questions will help you determine next steps:

- When did breach occur?
- Was my data compromised?
    - If so, what was accessed and how many records?
- Where did the breach occur?
- How and Why did it happen?

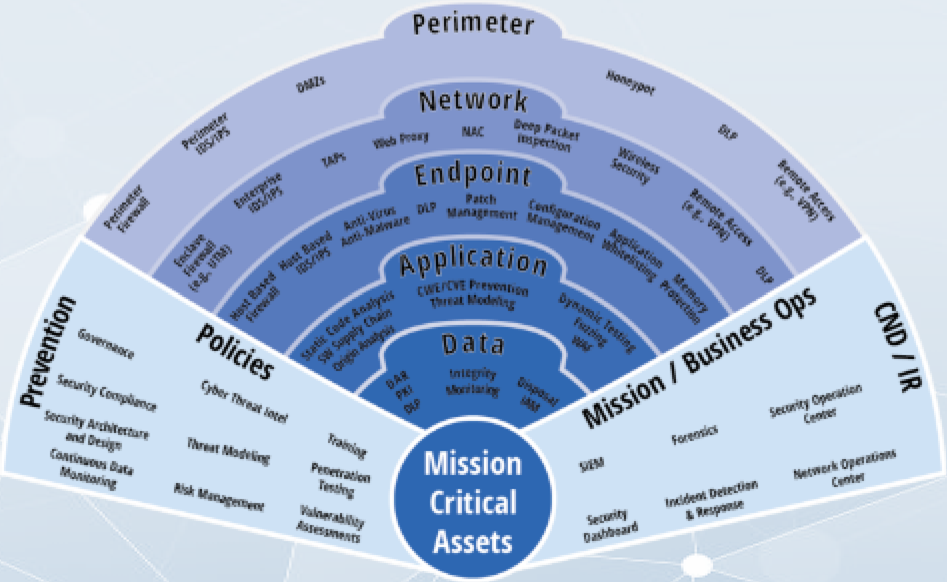
If confidential data was compromised (GLBA) you need to take action.

Digital Forensics

- If there's a possibility that customer information may have been compromised, you need to perform a Digital Forensic investigation
- Who performs – you or the vendor?
- Determine:
  - Who
  - What
  - Where
  - When
  - Why
  - How

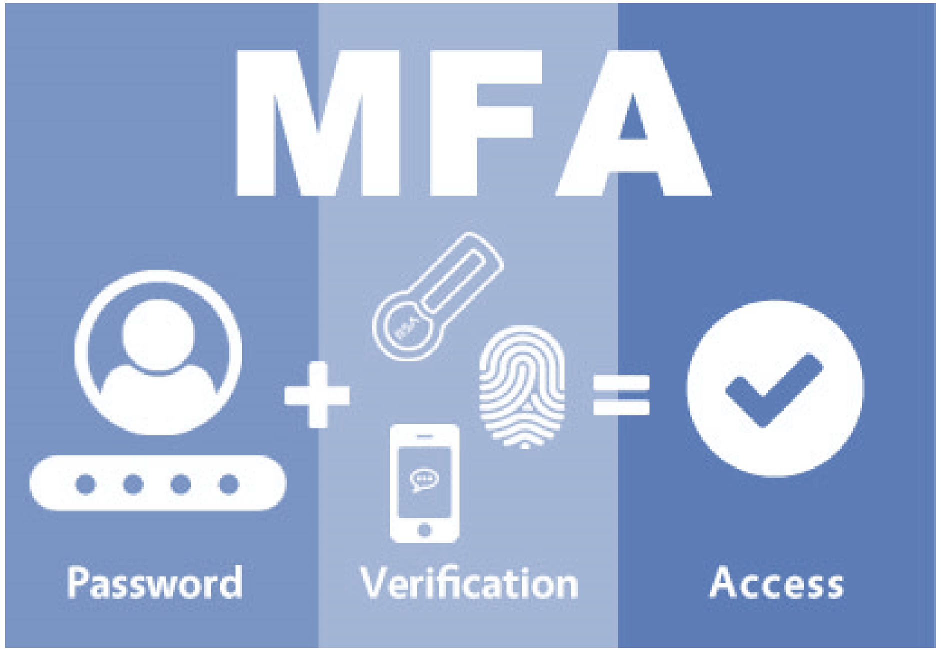
SBS INSTITUTE

Controls to Reduce Vendor Breach Risk



Necessary Controls

1. **Multi-Factor Authentication**
   - Deploy wherever possible, but a must for all internet-facing apps
2. **Strong Password Requirements**
   - Password Vault
   - Change Default Credentials
3. **Religious Patch Management**
4. **Weapons-Grade Data Backup**
   - Offsite and Immutable
5. **Network Segmentation/Isolation**
   - Internally and from vendor
6. **Egress Firewall Filtering**



DFIR Prep Checklist

- Developed by **SBS CyberSecurity**
- Highlights what orgs should have in place ahead of time to ensure both the ability to respond to an incident quickly AND perform a digital forensics investigation.
- https://sbscyber.com/resources/article-50-incident-response-preparedness-checklist-items

50+
Incident Response Preparedness Checklist Items

SBS institute

SBS CyberSecurity

www.sbscyber.com

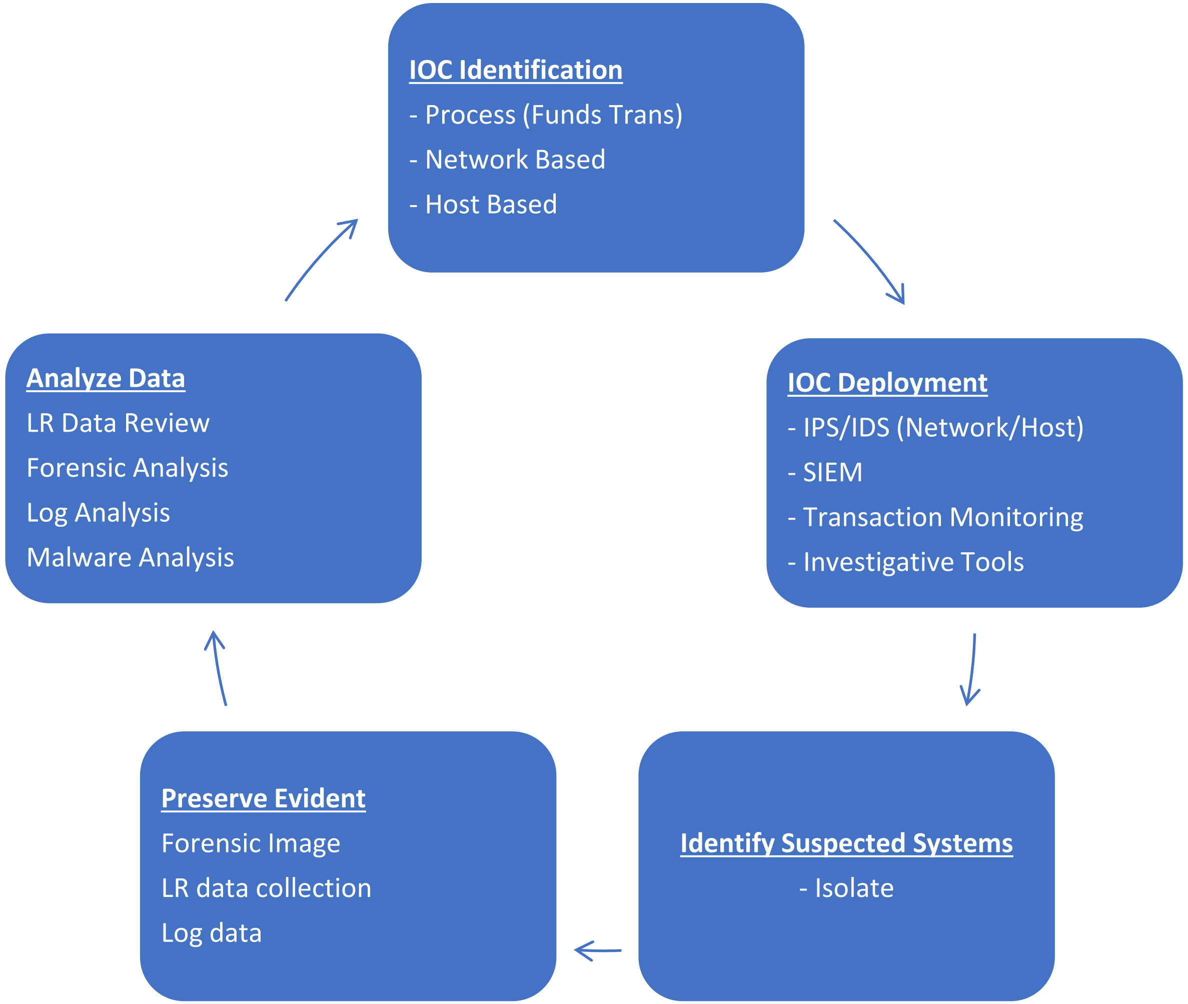
Written by: Buzz Hillestad, Senior Information Security Consultant at SBS CyberSecurity, LLC and Blake Coe, Vice President, Network Security at SBS CyberSecurity, LLC

Make sure you're logging the right stuff

At a minimum, monitor logs in these key areas:

- Total Network Logs per Second
- Patch Management % / Known Vulnerabilities
- Denied FTP Requests
- Denied Telnet Requests
- Failed Remote Logins
- VPN Connections / Failed VPN Connections
- Blacklisted IP Blocked
- Branch Connectivity Lost
- New Admin Credentials created
- Threshold for successive account lockouts
- VLAN ACL violations
- Changes to Group Policy
- Increase in network bandwidth
- Increase in outbound email traffic
- DNS Request anomalies

Indicators of Compromise (IoC)



IOC Identification

- Process (Funds Trans)
- Network Based
- Host Based

IOC Deployment

- IPS/IDS (Network/Host)
- SIEM
- Transaction Monitoring
- Investigative Tools

Identify Suspected Systems

- Isolate

Preserve Evident

Forensic Image

LR data collection

Log data

Analyze Data

LR Data Review

Forensic Analysis

Log Analysis

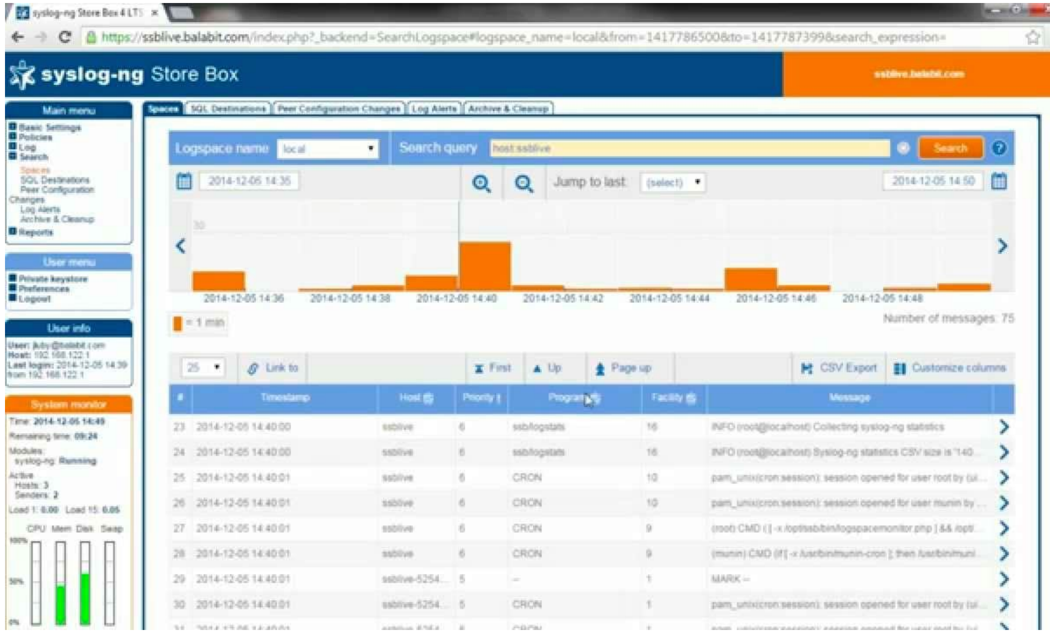
Malware Analysis

SBS BLOG POST: Indicators of Compromise: https://sbscyber.com/resources/indicators-of-compromise

http://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647?

Central Logging Capability

- This is not SIEM
- It is logging and log checking
- Make this server super protected from tampering – separate network segment?
  - Hardware firewall! Yes!
- Examples: syslog, syslog-ng, Snare, many others…
- See IR Prep Checklist



Logspace name: local

Search query: host:ssblive

2014-12-05 14:35 – 2014-12-05 14:50

Number of messages: 75

User info
User: judy@balabit.com
Host: 192.168.122.1
Last login: 2014-12-05 14:39 from 192.168.122.1

System monitor
Time: 2014-12-05 14:49
Remaining time: 09:24
Modules:
syslog-ng: Running
Active
Hosts: 3
Senders: 2
Load 1: 0.00 Load 15: 0.05
CPU Mem Disk Swap

#	Timestamp	Host	Priority	Program	Facility	Message
23	2014-12-05 14:40:00	ssblive	6	ssb/logstats	16	INFO (root@localhost) Collecting syslog-ng statistics
24	2014-12-05 14:40:00	ssblive	6	ssb/logstats	16	INFO (root@localhost) Syslog-ng statistics CSV size is '140...
25	2014-12-05 14:40:01	ssblive	6	CRON	10	pam_unix(cron:session): session opened for user root by (ui...
26	2014-12-05 14:40:01	ssblive	6	CRON	10	pam_unix(cron:session): session opened for user munin by ...
27	2014-12-05 14:40:01	ssblive	6	CRON	9	(root) CMD ([-x /opt/ssb/bin/logspacemonitor.php] && /opt/...
28	2014-12-05 14:40:01	ssblive	6	CRON	9	(munin) CMD (if [-x /usr/bin/munin-cron]; then /usr/bin/muni...
29	2014-12-05 14:40:01	ssblive-5254...	5	–	1	MARK --
30	2014-12-05 14:40:01	ssblive-5254...	5	CRON	1	pam_unix(cron:session): session opened for user root by (ui...

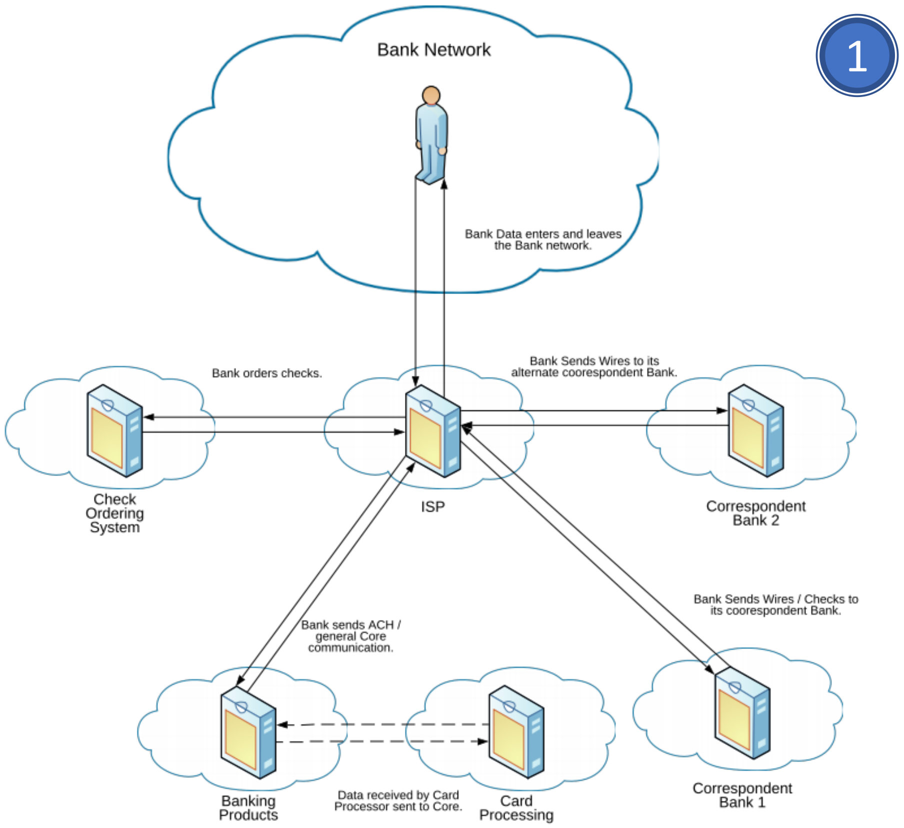
Separate User Accounts

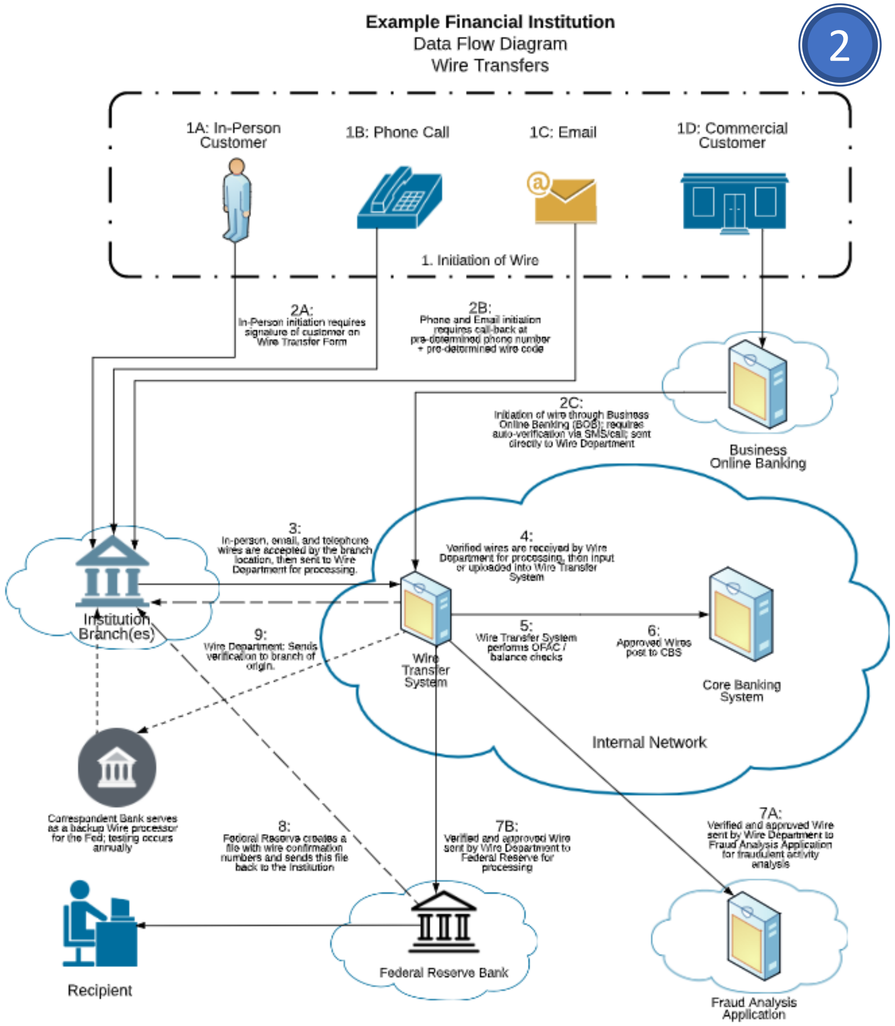
- **Accounts - Ultimate rule “one user, one account”**
  - Means accountability
  - All users should be restricted, ESPECIALLY vendors
  - Regular user accounts for EVERYONE; separate admin accounts for those that require such privileges
  - Ensure no one uses services accounts, you should know what their baseline looks like on your network
  - Ensure one the specific services uses its own service account

Network Protection - Order

1. **IDS**
2. **IPS**
3. **Logging**
   - Alerting
   - Limited Threat Hunting
4. **Honeypots**
5. **SIEM**
   - Automatic Threat Correlation
   - Threat Intelligence
   - Threat Hunting

Data Flow Diagrams


1
Bank Network
Bank Data enters and leaves the Bank network.
Bank orders checks.
Bank Sends Wires to its alternate coorespondent Bank.
Check Ordering System
ISP
Correspondent Bank 2
Bank Sends Wires / Checks to its coorespondent Bank.
Bank sends ACH / general Core communication.
Banking Products
Data received by Card Processor sent to Core.
Card Processing
Correspondent Bank 1


Example Financial Institution
Data Flow Diagram
Wire Transfers
2
1A: In-Person Customer
1B: Phone Call
1C: Email
1D: Commercial Customer
1. Initiation of Wire
2A: In-Person initiation requires signature of customer on Wire Transfer Form
2B: Phone and Email initiation requires call-back at pre-determined phone number + pre-determined wire code
2C: Initiation of wire through Business Online Banking (BOB); requires auto-verification via SMS/call; sent directly to Wire Department
Business Online Banking
Institution Branch(es)
3: In-person, email, and telephone wires are accepted by the branch location, then sent to Wire Department for processing.
4: Verified wires are received by Wire Department for processing, then input or uploaded into Wire Transfer System
Wire Transfer System
5: Wire Transfer System performs OFAC / balance checks
6: Approved Wires post to CBS
Core Banking System
9: Wire Department: Sends verification to branch of origin.
Internal Network
Correspondent Bank serves as a backup Wire processor for the Fed; testing occurs annually
8: Federal Reserve creates a file with wire confirmation numbers and sends this file back to the Institution
7B: Verified and approved Wire sent by Wire Department to Federal Reserve for processing
7A: Verified and approved Wire sent by Wire Department to Fraud Analysis Application for fraudulent activity analysis
Recipient
Federal Reserve Bank
Fraud Analysis Application

SBS BLOG POST: Data Flow Diagrams
https://sbscyber.com/resources/data-flow-diagrams-101

Cyber Insurance Exclusions

- As cyber insurance companies continue to pay out for cyber crime (200% increase in pay-outs from 2018-2021), limits and exclusions continue to be made to cyber insurance policies
- Common exclusions of cyber insurance policies include:
  - Third-party providers (**vendor or supply-chain breaches**)
  - Lost or stolen (portable) devices
  - Acts of war, invasion, or terrorism (**state-sponsored actors are now commonly included in this exclusion**)
  - Failure to Maintain (**not meeting minimum security standards** approved by the cyber insurance provider)
  - Lost revenue resulting from a cyber attack (insurance company may cover some/all of the expense to recover, but **not necessarily lost revenue**)
- Cyber insurance and carriers are still evolving… **be aware**!

Cyber Crime Cost Statistics

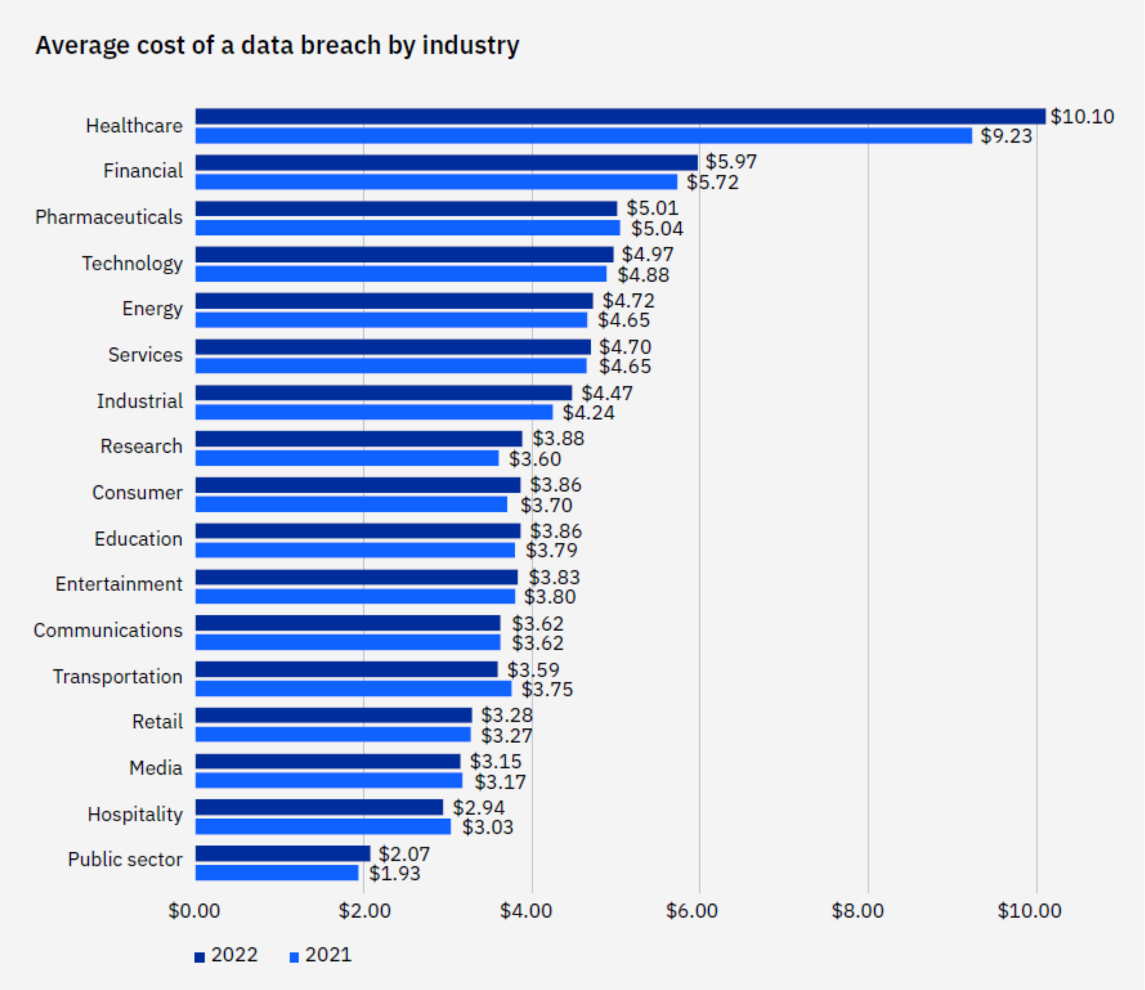


Figure 4: Measured in USD millions

IBM/Ponemon Annual Cost of a Data Breach Report 2022: https://www.ibm.com/reports/data-breach

- Global average cost of a data breach: $4.35 million in 2022
- **US average cost of a data breach: $9.44 million in 2022**
- Global per-record cost of a data breach: $164 in 2022
- Healthcare breaches were far-and-away the most expensive
- Financial breaches were the second-most costly

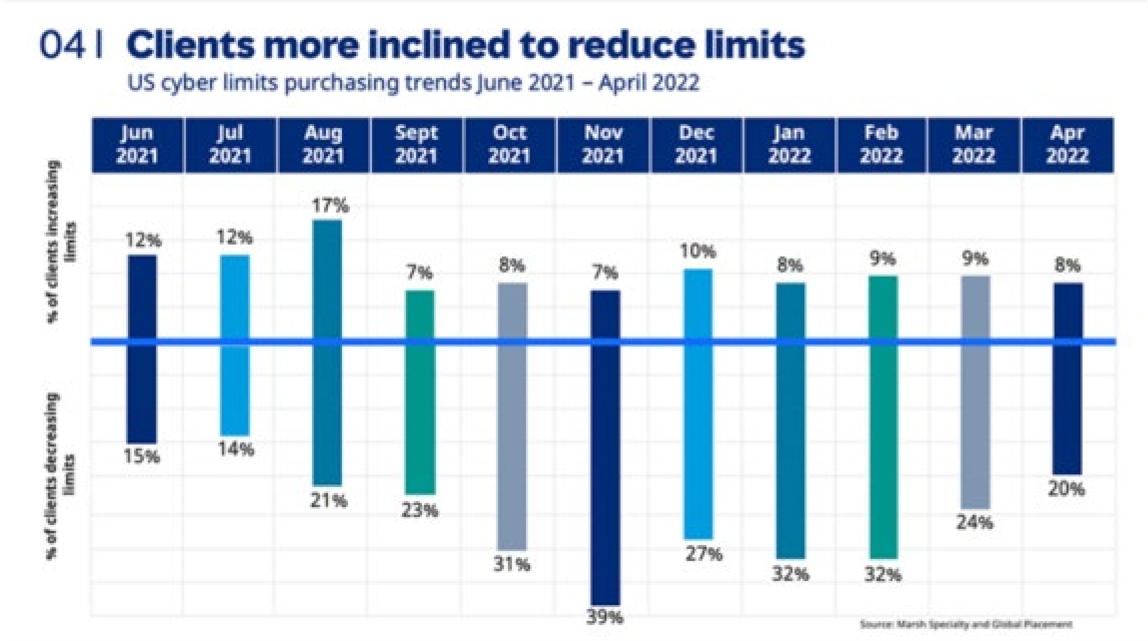
Cyber Insurance Statistics

- 27% of data breach claims and 24% of first-party claims had some exclusion written into the policy that prevented part-payout or full-payout.
- In a 2022 survey, only 19% of organizations claimed to have coverage for cyber events beyond $600,000.
- Only 55% of organizations claimed to have any cybersecurity insurance at all.
- In the past 3 years, cyber insurance claims have increased by an order of 100% and payouts a total of 200%, with the peak claims being 8,100 in 2021.
- 99% of all cybersecurity insurance claims came from SME companies (annual revenue under $2 billion).
- The average cybersecurity insurance claim cost for a small to medium enterprise is $345,000.
- The average cybersecurity insurance claim cost for an SME for a ransomware event is $485,000. The average claim for all organizations is $812,360.

https://networkassured.com/security/cybersecurity-insurance-statistics/

Cyber Insurance Pricing

- According to the Global Insurance Market Index, insurance broker Marsh stated rise in 2022:
  - 28% in Q4
  - 48% in Q3
  - 79% in Q2
- Insurance clients have tended to reduce limits over the past 2 years to compensate for increases in premiums
- Premiums are beginning to re-stabilize
- Cost of compliance still increasing



04 | Clients more inclined to reduce limits

US cyber limits purchasing trends June 2021 – April 2022

Source: Marsh Specialty and Global Placement

Top Cyber Insurance Requirements 2023

- Expectations of strong security are increasing, including
  - **Multi-Factor Authentication (MFA) for admin accounts**
  - Endpoint Detection & Response (EDR)
  - Managed Detection & Response (MDR – outsourced SOC)
  - **Strong Patch Management Program**
  - **Secured Data Backups and DR Plan**
  - **Incident Response Plan (and testing)**
  - No End-of-Life Software
  - Dark Web Monitoring
  - **Employee Training**
  - **Vulnerability Management (regular VA scans)**
  - **Vendor Management**

Cyber Insurance Exclusions

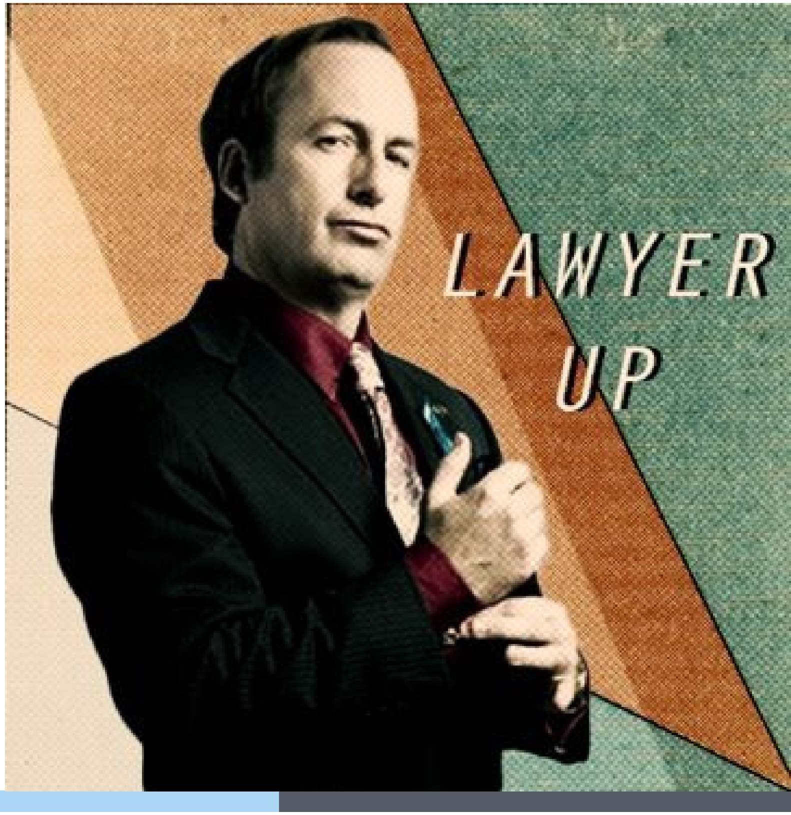
- As cyber insurance companies continue to pay out for cyber crime (200% increase in pay-outs from 2018-2021), limits and exclusions continue to be made to cyber insurance policies
- Common exclusions of cyber insurance policies include:
  - Third-party providers (**vendor or supply-chain breaches**)
  - Lost or stolen (portable) devices
  - Acts of war, invasion, or terrorism (**state-sponsored actors are now commonly included in this exclusion**)
  - Failure to Maintain (**not meeting minimum security standards** approved by the cyber insurance provider)
  - Lost revenue resulting from a cyber attack (insurance company may cover some/all of the expense to recover, but **not necessarily lost revenue**)
- Cyber insurance and carriers are still evolving… **be aware**!

Insurance

- **Do you have proper cyber insurance coverage in place?**
  - Cyber Insurance is in a tricky spot right now… there's NO STANDARD
  - Do you know your options? Does it include coverage for a vendor breach?
  - Do you know what's REALLY covered? Watch out for **EXCLUSIONS!**
  - What do insurance companies expect from YOUR cybersecurity controls before paying the claim?
  - Does your coverage include Incident Response and Digital Forensics coverage?
  - **Check with your insurance company about who can/will help**

Legal

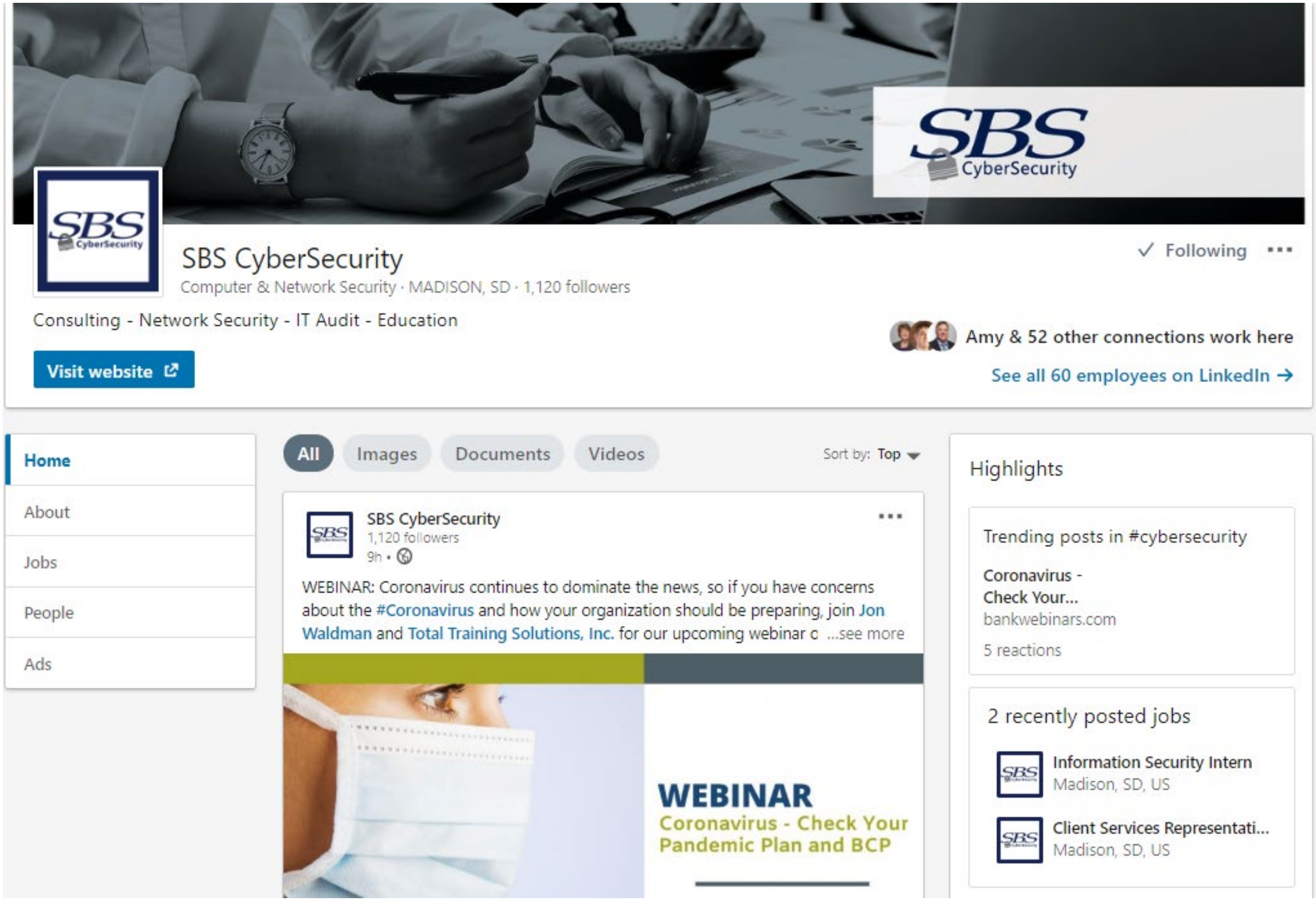
- Engaging your legal team can help protect your organization, especially if an investigation is needed
  - Hint: it usually is
- Run communication through legal team
- Engage with law enforcement
- Attorney-client privilege
- Determine if/when to notify customers
- Negotiate the ransom…?



We’re more reliant on vendors than ever…

- **… Just remember, you’re the customer, and it’s YOUR data**
- It’s your responsibility to protect your customer information, your employees, and your institution no matter where the data resides
- Your vendor is not going to notify your customers of a breach for you… or take the blame
- Understand your Vendor’s security practices
- Align Vendors with your cybersecurity goals and standards
- **It’s your responsibility to ensure the protection of your data**

SBS on LinkedIn



SBS CyberSecurity

Computer & Network Security · MADISON, SD · 1,120 followers

Consulting - Network Security - IT Audit - Education

✓ Following ···

Amy & 52 other connections work here

See all 60 employees on LinkedIn →

SBS CyberSecurity
1,120 followers
9h •

WEBINAR: Coronavirus continues to dominate the news, so if you have concerns about the #Coronavirus and how your organization should be preparing, join Jon Waldman and Total Training Solutions, Inc. for our upcoming webinar o ...see more

Highlights

Trending posts in #cybersecurity

Coronavirus - Check Your...
bankwebinars.com
5 reactions

2 recently posted jobs

Information Security Intern
Madison, SD, US

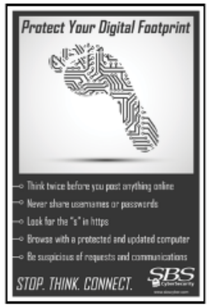
Client Services Representati...
Madison, SD, US

https://www.linkedin.com/company/sbs-cybersecurity

Complimentary Resources

POSTERS

Click on the image to download your security awareness poster.


Protect Your Digital Footprint

- Think twice before you post anything online
- Never share usernames or passwords
- Look for the "s" in https
- Browse with a protected and updated computer
- Be suspicious of requests and communications

STOP. THINK. CONNECT. SBS CyberSecurity

DON'T GET HOOKED

PROTECT YOURSELF FROM PHISHING SCAMS

Security Alert

A hacker may have your password!

- Never use a common password for multiple accounts
- Always use multifactor authentication
- Change your password often
- Never share your password
- Store your passwords securely

Accept

DON'T TAKE THE BAIT!

INFOGRAPHICS

Click on the image below to download the Infographic.

The SBS Risk Management Method

How to make Risk Management be your BEST FRIEND!

1 When it comes to anything new, EVERYTHING should start with the...

RISK ASSESSMENT!

2 Your Risk Assessment needs to help you make...

DECISIONS!

10 Key Ideas to Build a CYBERSECURITY CULTURE

01 START AT THE TOP WITH THE BOARD

02 GIVE CYBERSECURITY A STANDING AGENDA ITEM AT EMPLOYEE MEETINGS

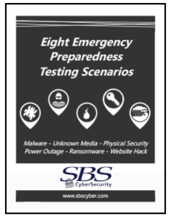
Ransomware Toolkit

ATM Assurance Toolkit

RESOURCE LIBRARY

SBS is your resource for cybersecurity tips, tricks, and best practice guides to help support the cybersecurity culture at your organization. Click the image to download your guide.

FDIC InTREx: What Documentation Are You Expected to Have?


Eight Emergency Preparedness Testing Scenarios

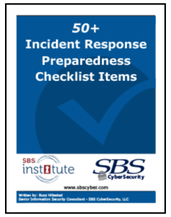
Malware - Unknown Media - Physical Security Power Outage - Ransomware - Website Hack

www.sbscyber.com

Defense in Depth Checklist Controls

50 Easy-to-Implement Controls to Strengthen Your Security

www.sbscyber.com


50+ Incident Response Preparedness Checklist Items

www.sbscyber.com

34 Unique Ideas to Create a Culture of Cybersecurity

Brought to you by:

www.sbscyber.com

You Are a Technology Company

Three steps to changing your view

www.sbscyber.com

18 CYBERSECURITY TIPS

Ten Essential Cybersecurity Best Practices

Banking • Business • Employees

www.sbscyber.com

Cybersecurity Starter Toolkit

Cybersecurity Advanced Toolkit

https://sbscyber.com/education/free-downloads

Contact Information

SBS CyberSecurity

Follow us on Social:

Terry Kuxhaus (CISSP)

- Senior IS Consultant/Regional Director
- Bachelors of Science in Technology for Black Hills State University
- Terry.kuxhaus@sbscyber.com
- 605-222-7400
- www.sbscyber.com

SBS Institute

- sbsinstitute@sbscyber.com
- 605-269-0909

SBS CyberSecurity

Understand risk.
Make intelligent decisions.