networking
We design and support business networks by project or SPOT Managed.

security
Let us enhance your security posture with policies, auditing or tools.

voip
Empower your phones with lower costs and more functionality.

storage
Explore the benefits of centralized storage and make life easier.

dr/bc
We can keep critical systems, servers, and WAN links more available.

services
Get advanced benefits from hosted services.

Incident Response Planning

Tips and Resources

THE FULCRUM GROUP
One Technology Solution: Yours

Presented by
Steve "The Doctor" Meek, CISSP

LinkedIn:
https://www.linkedin.com/in/stevemeekcissp/

Twitter:
https://twitter.com/TheFulcrumGroup

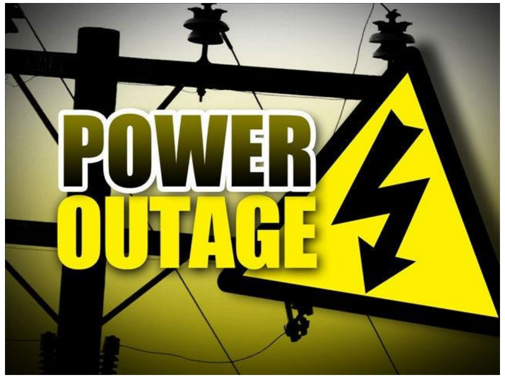
Email:
steve@fulcrumgroup.net

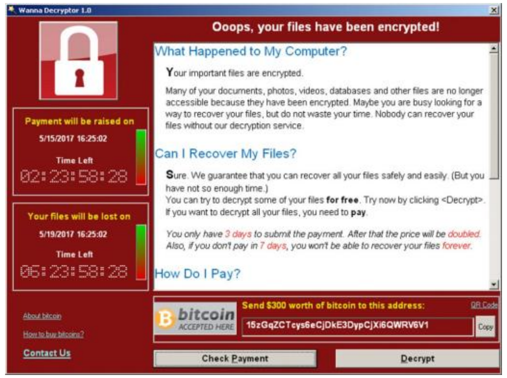
Agenda

- Why?
- Get Started
- Build Your Team
- Resources
- Incident Response Framework
- Attack Scenarios
- Recovery Procedures
- Testing
- Summary

Why?

- Cyberinsurance?
- Impact
- Risk of a breach
- Compliance
- Reputation
- Collaborate
- Time and resources




Wanna Decryptor 1.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

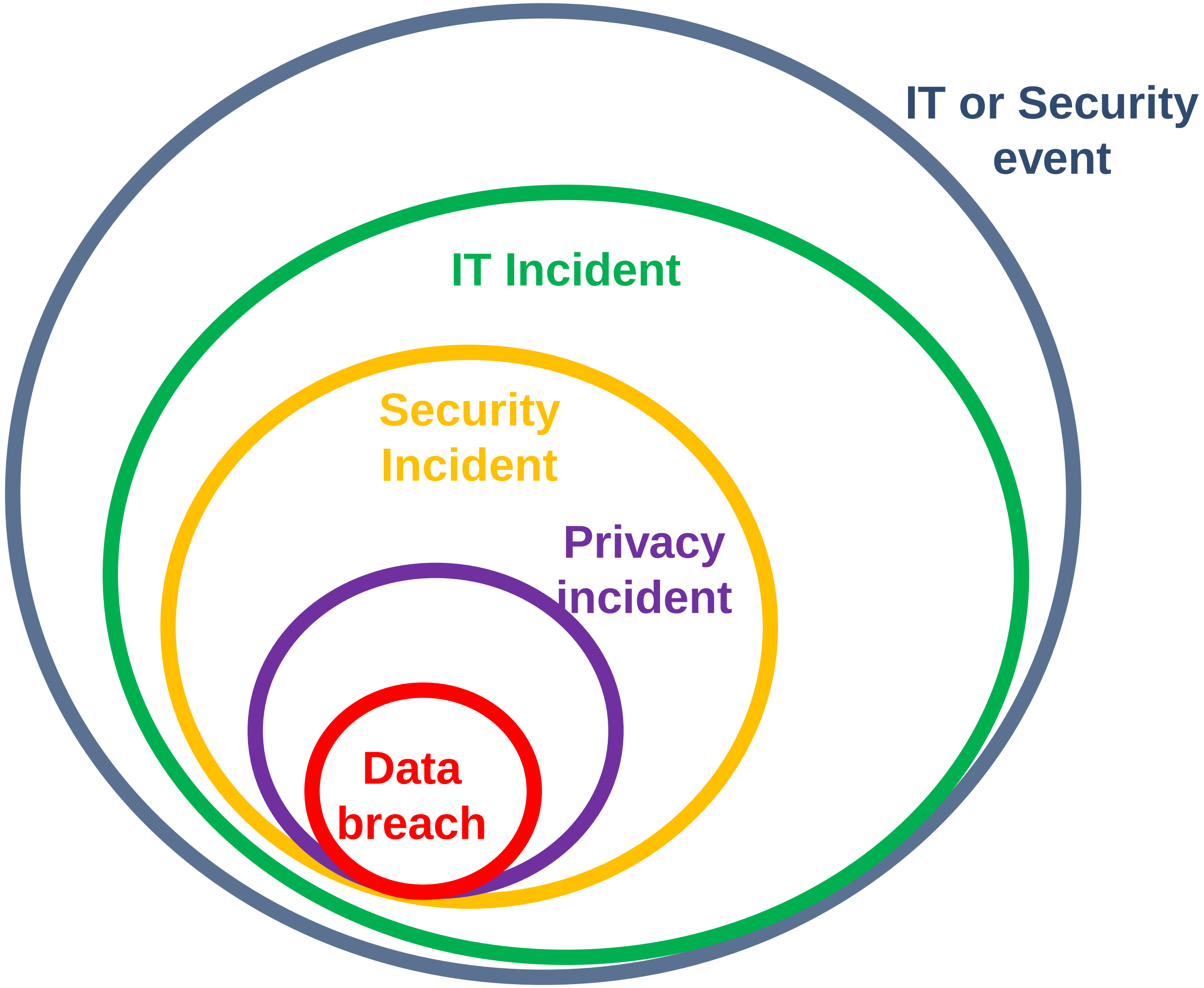
Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28

Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28

Send $300 worth of bitcoin to this address:
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Why?

- Events (always start here)
- Incidents
- Breaches



IT or Security event

IT Incident

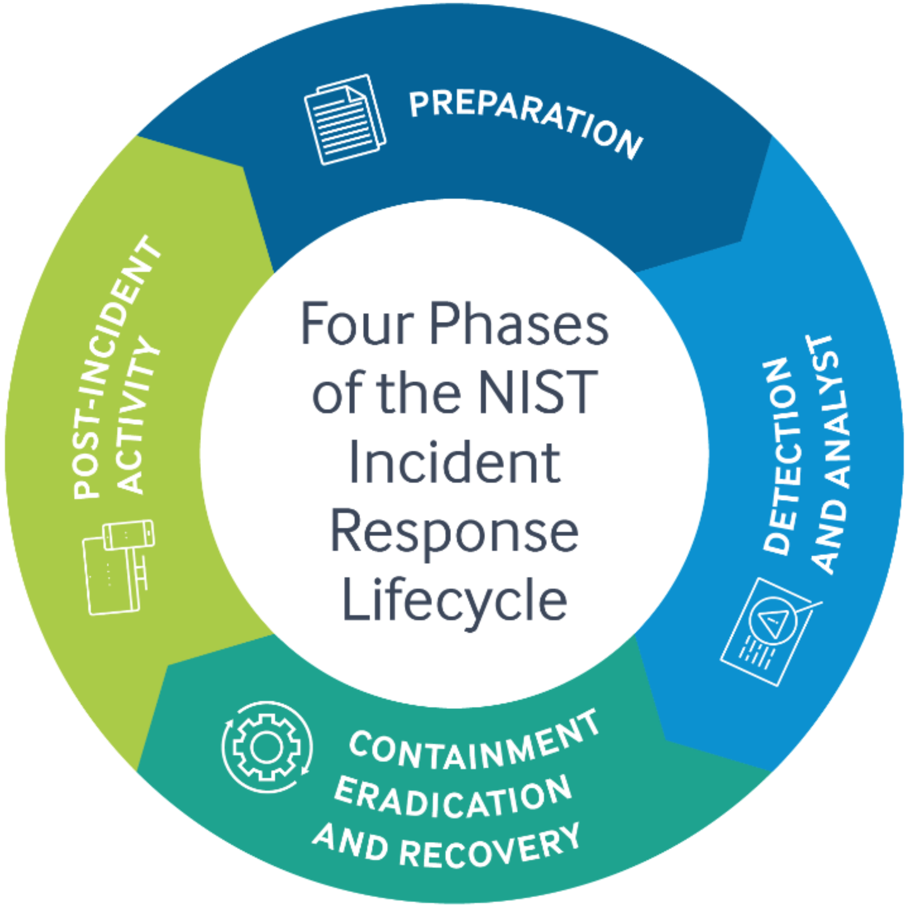
Security Incident

Privacy incident

Data breach

Getting Started

- Team
- Scope
- Risks
- Response Process
- Assign Roles
- Communication
- Testing
- Training

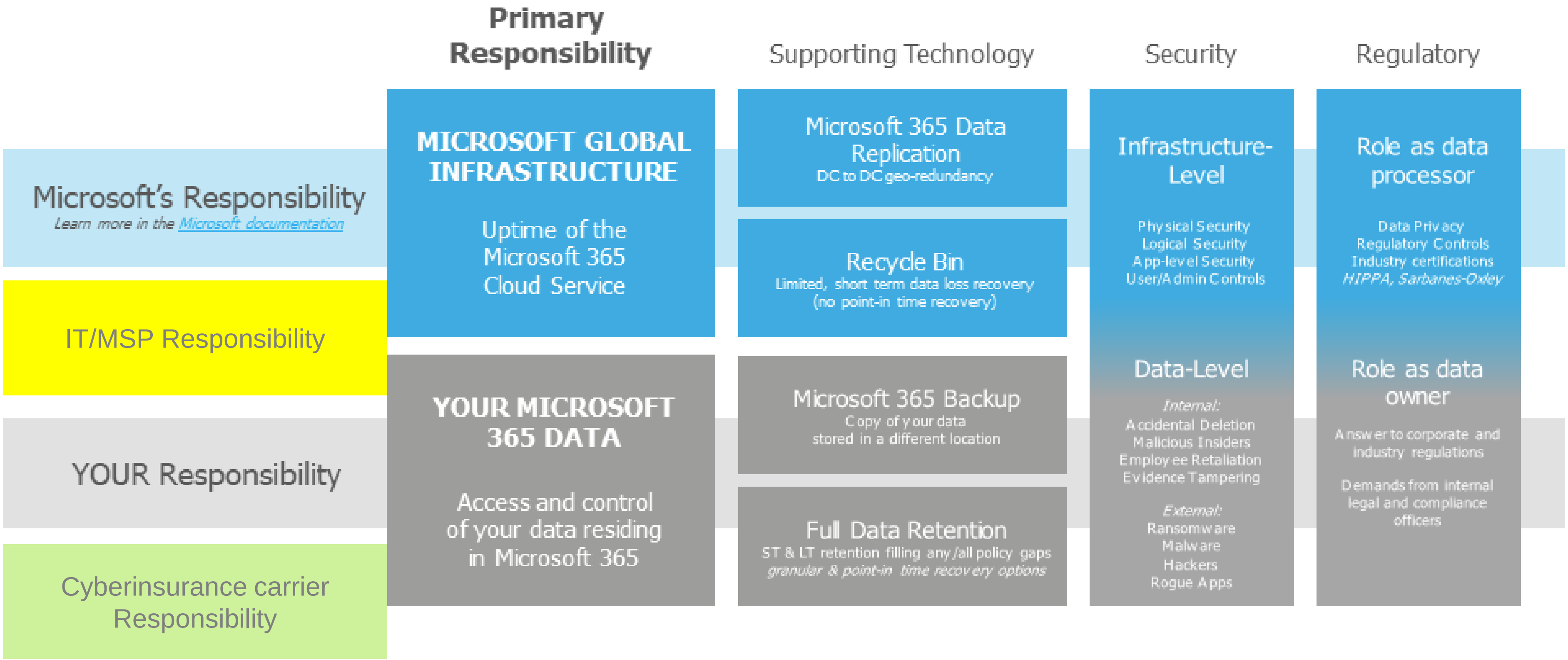

PREPARATION
DETECTION AND ANALYST
CONTAINMENT ERADICATION AND RECOVERY
POST-INCIDENT ACTIVITY
Four Phases of the NIST Incident Response Lifecycle

Build Your Team

- Roles
- Team Members
- Procedures
- Training
- Communication
- Severity Levels
- Partners

Build Your Team

The Microsoft 365 Shared Responsibility Model



Primary Responsibility

Supporting Technology

Security

Regulatory

Microsoft's Responsibility
Learn more in the Microsoft documentation

IT/MSP Responsibility

YOUR Responsibility

Cyberinsurance carrier Responsibility

MICROSOFT GLOBAL INFRASTRUCTURE

Uptime of the Microsoft 365 Cloud Service

YOUR MICROSOFT 365 DATA

Access and control of your data residing in Microsoft 365

Microsoft 365 Data Replication
DC to DC geo-redundancy

Recycle Bin
Limited, short term data loss recovery
(no point-in time recovery)

Microsoft 365 Backup
Copy of your data
stored in a different location

Full Data Retention
ST & LT retention filling any/all policy gaps
granular & point-in time recovery options

Infrastructure-Level

Physical Security
Logical Security
App-level Security
User/Admin Controls

Data-Level

Internal:
Accidental Deletion
Malicious Insiders
Employee Retaliation
Evidence Tampering

External:
Ransomware
Malware
Hackers
Rogue Apps

Role as data processor

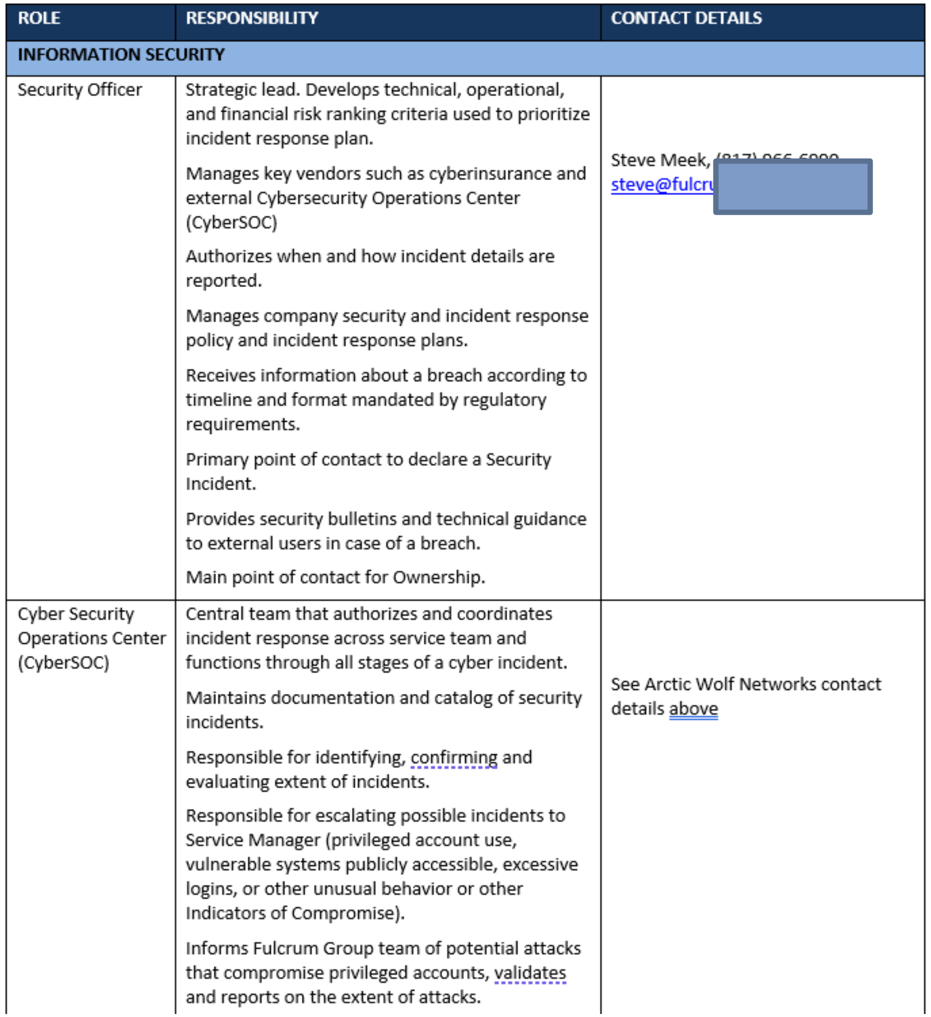
Data Privacy
Regulatory Controls
Industry certifications
HIPPA, Sarbanes-Oxley

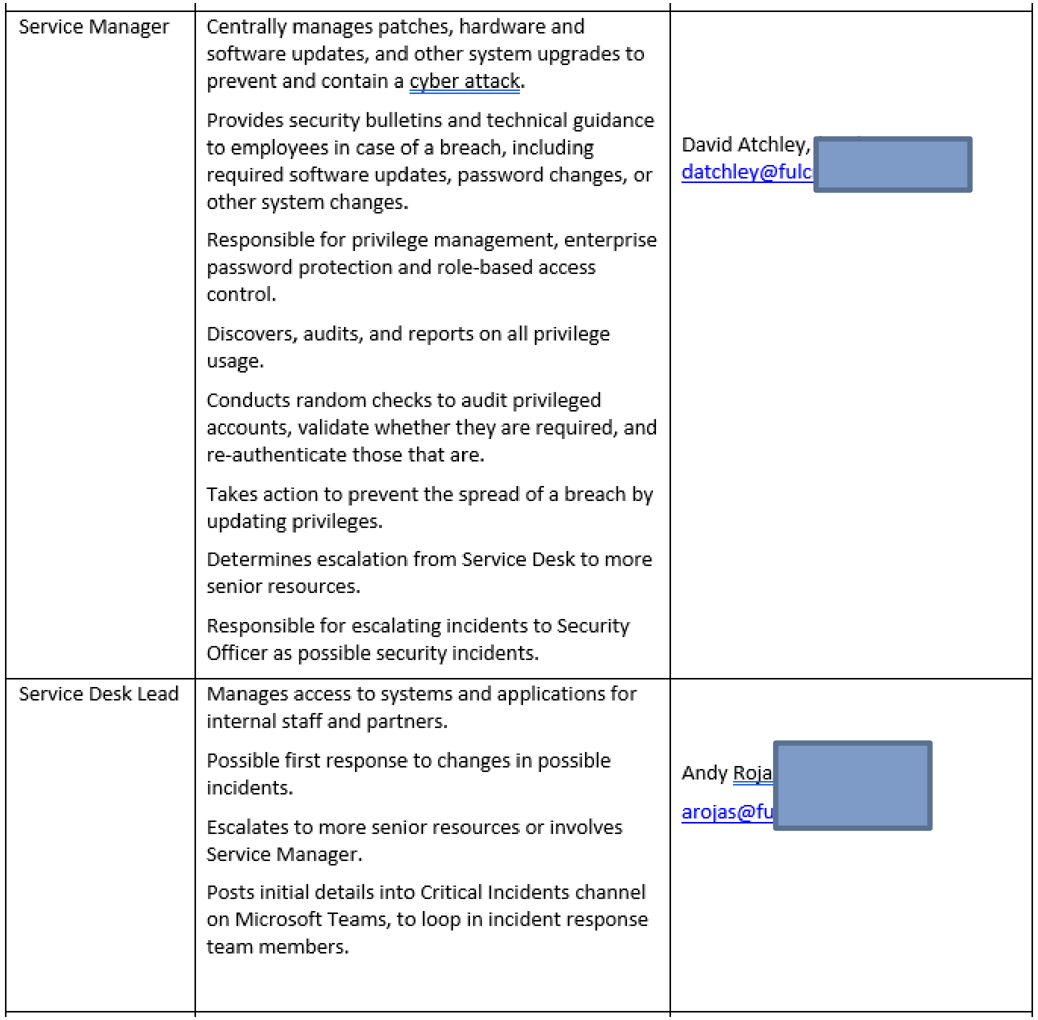
Role as data owner

Answer to corporate and industry regulations

Demands from internal legal and compliance officers

Build Your Team



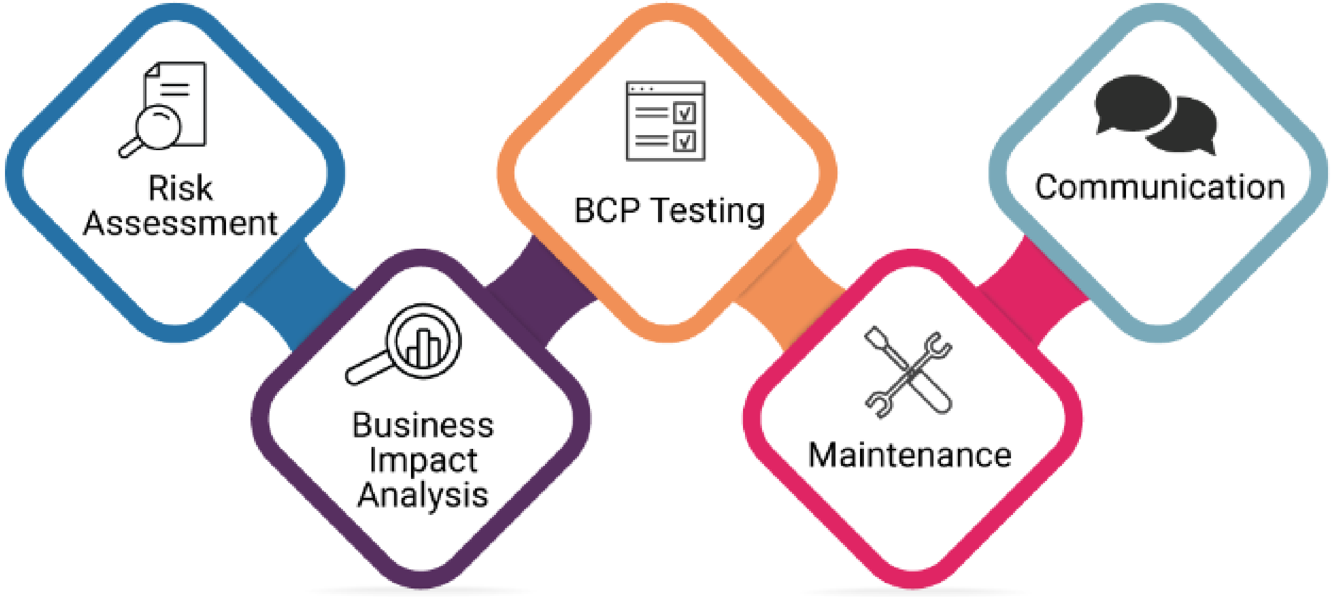


ROLE	RESPONSIBILITY	CONTACT DETAILS
INFORMATION SECURITY		
Security Officer	Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plan. Manages key vendors such as cyberinsurance and external Cybersecurity Operations Center (CyberSOC) Authorizes when and how incident details are reported. Manages company security and incident response policy and incident response plans. Receives information about a breach according to timeline and format mandated by regulatory requirements. Primary point of contact to declare a Security Incident. Provides security bulletins and technical guidance to external users in case of a breach. Main point of contact for Ownership.	Steve Meek, [redacted] steve@fulcru
Cyber Security Operations Center (CyberSOC)	Central team that authorizes and coordinates incident response across service team and functions through all stages of a cyber incident. Maintains documentation and catalog of security incidents. Responsible for identifying, confirming and evaluating extent of incidents. Responsible for escalating possible incidents to Service Manager (privileged account use, vulnerable systems publicly accessible, excessive logins, or other unusual behavior or other Indicators of Compromise). Informs Fulcrum Group team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks.	See Arctic Wolf Networks contact details above
Service Manager	Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyber attack. Provides security bulletins and technical guidance to employees in case of a breach, including required software updates, password changes, or other system changes. Responsible for privilege management, enterprise password protection and role-based access control. Discovers, audits, and reports on all privilege usage. Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are. Takes action to prevent the spread of a breach by updating privileges. Determines escalation from Service Desk to more senior resources. Responsible for escalating incidents to Security Officer as possible security incidents.	David Atchley, [redacted] datchley@fulc
Service Desk Lead	Manages access to systems and applications for internal staff and partners. Possible first response to changes in possible incidents. Escalates to more senior resources or involves Service Manager. Posts initial details into Critical Incidents channel on Microsoft Teams, to loop in incident response team members.	Andy Roja [redacted] arojas@fu

THE FULCRUM GROUP
One Technology Solution: Yours

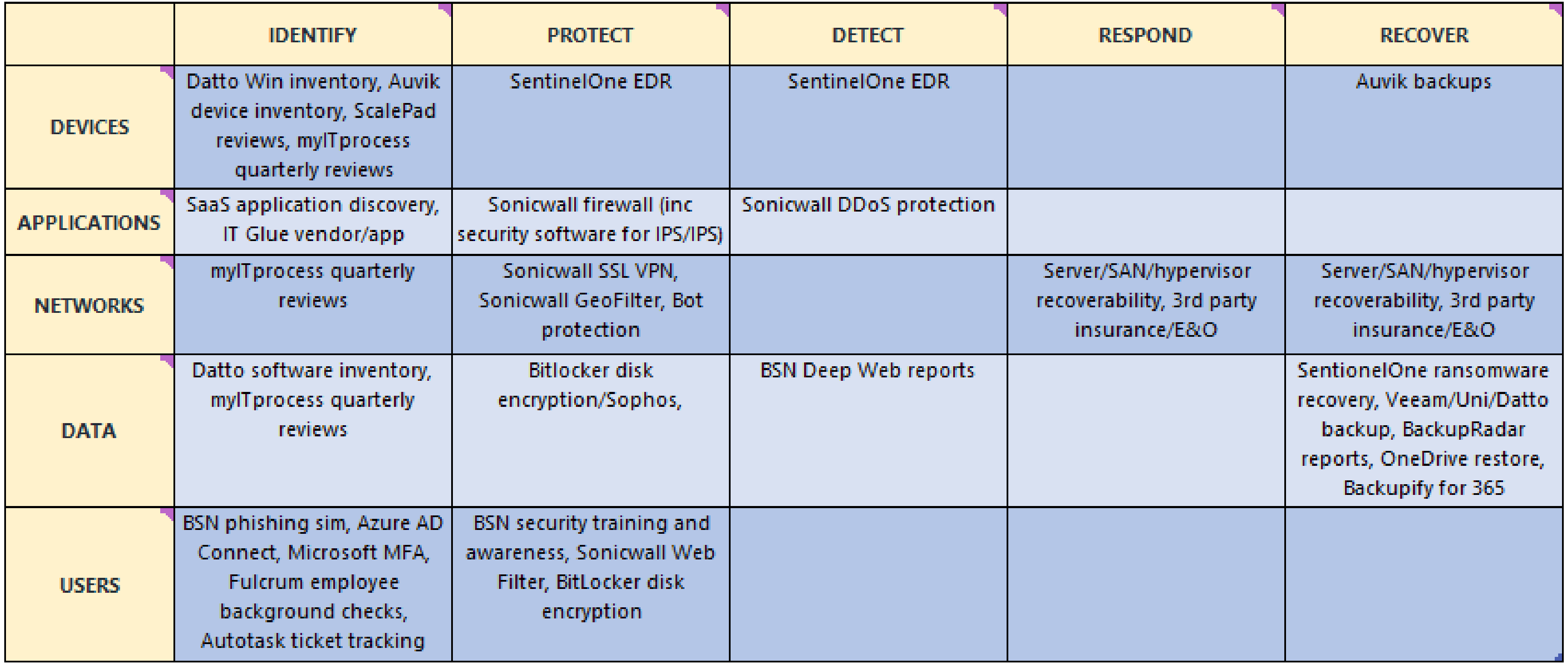
Prep Work

- Critical Assets and Data
- Risks
- Incident Types
- Procedures
- Contacts
- Communication Plans
- Partners
- Exercises



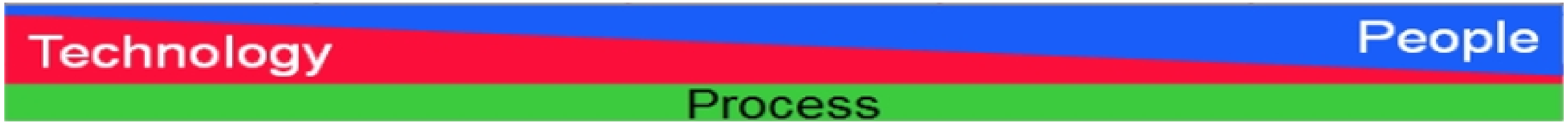
Prep Work

Fulcrum Cyber Defense Matrix

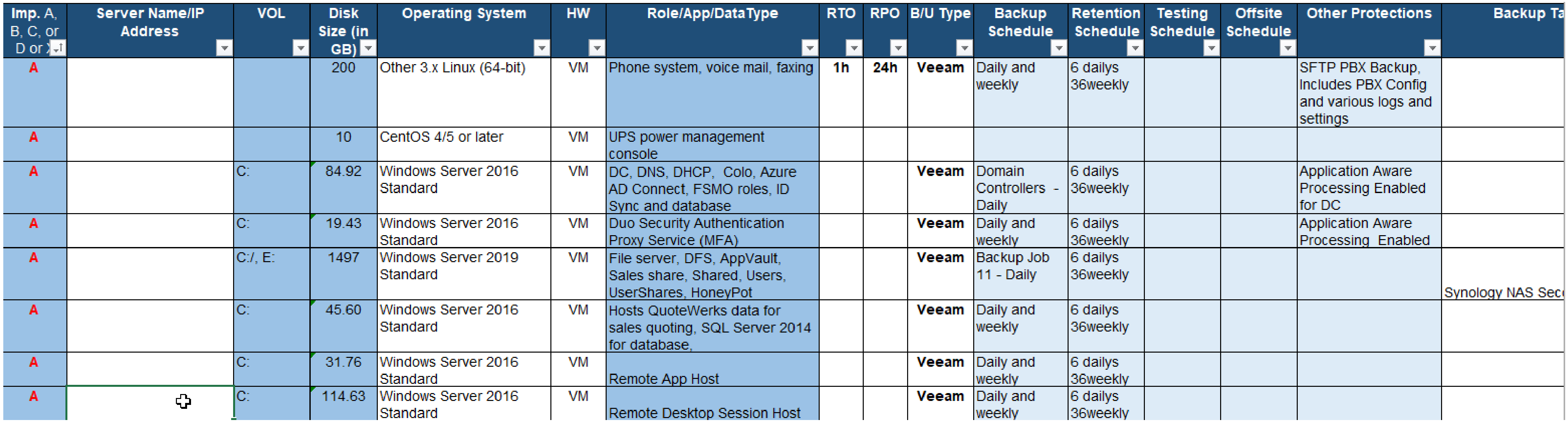


	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DEVICES	Datto Win inventory, Auvik device inventory, ScalePad reviews, myITprocess quarterly reviews	SentinelOne EDR	SentinelOne EDR		Auvik backups
APPLICATIONS	SaaS application discovery, IT Glue vendor/app	Sonicwall firewall (inc security software for IPS/IPS)	Sonicwall DDoS protection		
NETWORKS	myITprocess quarterly reviews	Sonicwall SSL VPN, Sonicwall GeoFilter, Bot protection		Server/SAN/hypervisor recoverability, 3rd party insurance/E&O	Server/SAN/hypervisor recoverability, 3rd party insurance/E&O
DATA	Datto software inventory, myITprocess quarterly reviews	Bitlocker disk encryption/Sophos,	BSN Deep Web reports		SentionelOne ransomware recovery, Veeam/Uni/Datto backup, BackupRadar reports, OneDrive restore, Backupify for 365
USERS	BSN phishing sim, Azure AD Connect, Microsoft MFA, Fulcrum employee background checks, Autotask ticket tracking	BSN security training and awareness, Sonicwall Web Filter, BitLocker disk encryption			

Degree of Dependency



Prep Work

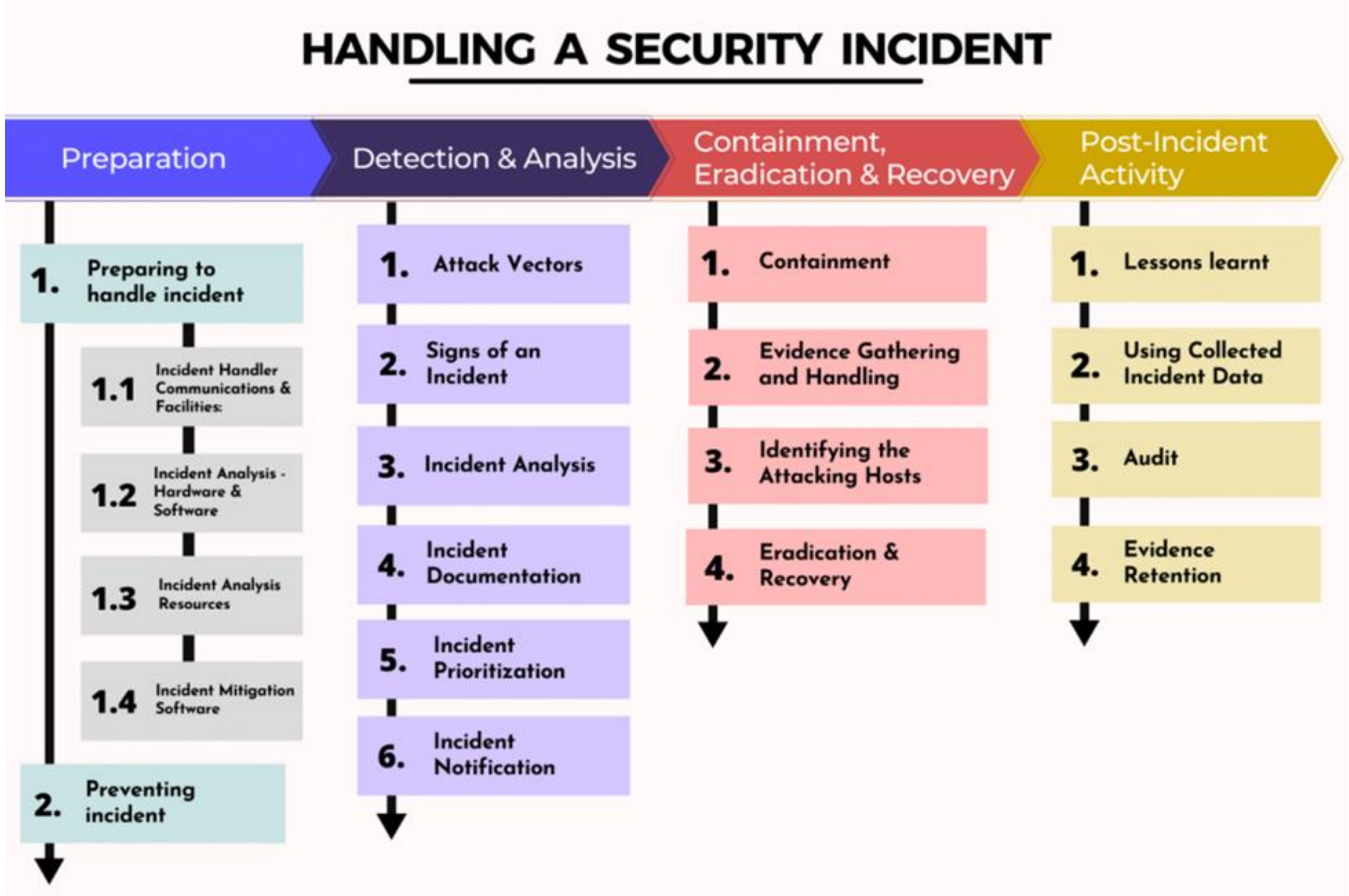


Imp. A, B, C, or D or X	Server Name/IP Address	VOL	Disk Size (in GB)	Operating System	HW	Role/App/DataType	RTO	RPO	B/U Type	Backup Schedule	Retention Schedule	Testing Schedule	Offsite Schedule	Other Protections	Backup Ta
A			200	Other 3.x Linux (64-bit)	VM	Phone system, voice mail, faxing	1h	24h	Veeam	Daily and weekly	6 dailys 36weekly			SFTP PBX Backup, Includes PBX Config and various logs and settings	
A			10	CentOS 4/5 or later	VM	UPS power management console									
A		C:	84.92	Windows Server 2016 Standard	VM	DC, DNS, DHCP, Colo, Azure AD Connect, FSMO roles, ID Sync and database			Veeam	Domain Controllers - Daily	6 dailys 36weekly			Application Aware Processing Enabled for DC	
A		C:	19.43	Windows Server 2016 Standard	VM	Duo Security Authentication Proxy Service (MFA)			Veeam	Daily and weekly	6 dailys 36weekly			Application Aware Processing Enabled	
A		C:/, E:	1497	Windows Server 2019 Standard	VM	File server, DFS, AppVault, Sales share, Shared, Users, UserShares, HoneyPot			Veeam	Backup Job 11 - Daily	6 dailys 36weekly				Synology NAS Sec
A		C:	45.60	Windows Server 2016 Standard	VM	Hosts QuoteWerks data for sales quoting, SQL Server 2014 for database,			Veeam	Daily and weekly	6 dailys 36weekly				
A		C:	31.76	Windows Server 2016 Standard	VM	Remote App Host			Veeam	Daily and weekly	6 dailys 36weekly				
A		C:	114.63	Windows Server 2016 Standard	VM	Remote Desktop Session Host			Veeam	Daily and weekly	6 dailys 36weekly				

THE FULCRUM GROUP
One Technology Solution: Yours

Incident Response Framework

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Analysis
- Post-incident



HANDLING A SECURITY INCIDENT

Preparation

1. Preparing to handle incident
   - 1.1 Incident Handler Communications & Facilities:
   - 1.2 Incident Analysis - Hardware & Software
   - 1.3 Incident Analysis Resources
   - 1.4 Incident Mitigation Software
2. Preventing incident

Detection & Analysis

1. Attack Vectors
2. Signs of an Incident
3. Incident Analysis
4. Incident Documentation
5. Incident Prioritization
6. Incident Notification

Containment, Eradication & Recovery

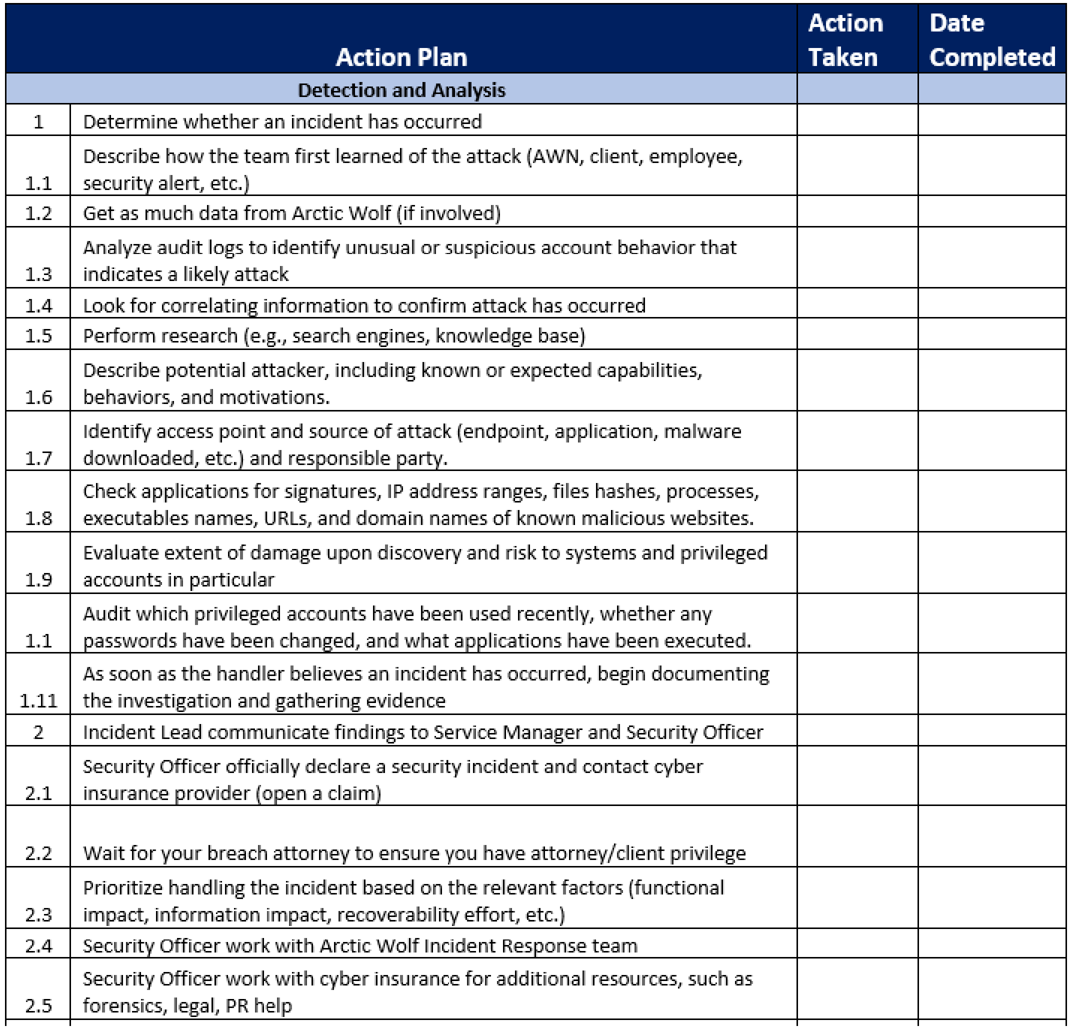
1. Containment
2. Evidence Gathering and Handling
3. Identifying the Attacking Hosts
4. Eradication & Recovery

Post-Incident Activity

1. Lessons learnt
2. Using Collected Incident Data
3. Audit
4. Evidence Retention

For ChatGPT, sign up at official website of OpenAI at https://chat.openai.com/auth/login

Incident Response Framework



Action Plan		Action Taken	Date Completed
	Detection and Analysis		
1	Determine whether an incident has occurred		
1.1	Describe how the team first learned of the attack (AWN, client, employee, security alert, etc.)		
1.2	Get as much data from Arctic Wolf (if involved)		
1.3	Analyze audit logs to identify unusual or suspicious account behavior that indicates a likely attack		
1.4	Look for correlating information to confirm attack has occurred		
1.5	Perform research (e.g., search engines, knowledge base)		
1.6	Describe potential attacker, including known or expected capabilities, behaviors, and motivations.		
1.7	Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party.		
1.8	Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites.		
1.9	Evaluate extent of damage upon discovery and risk to systems and privileged accounts in particular		
1.1	Audit which privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed.		
1.11	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence		
2	Incident Lead communicate findings to Service Manager and Security Officer		
2.1	Security Officer officially declare a security incident and contact cyber insurance provider (open a claim)		
2.2	Wait for your breach attorney to ensure you have attorney/client privilege		
2.3	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)		
2.4	Security Officer work with Arctic Wolf Incident Response team		
2.5	Security Officer work with cyber insurance for additional resources, such as forensics, legal, PR help		

Items Gathered During An Incident

- Logs considered to be very significant: Firewall, Event logs, Active Directory
- Logs considered to be significant: DNS, Web Proxy, Remote Access Authentication, DHCP lease, router, IDS/IPS alerts, endpoint security (Antivirus, Antimalware), VPN, two-factor authentication, SNMP, SIEM
- Live forensic image of RAM and virtualized RAM (if available, also a back-up copy for Delta Analysis) on compromised client or servers
- Live image of breached servers (not storage pools), to include remote, third-party and cloud servers, either as a full export or a back-up copy of the server in its current state
- Timeline of events
- Physical and virtual network topology
- Copy of malware or tools used by suspected offenders
- Copies of emails suspected to be malicious with full headers and attachments
- Copies of links suspected of causing the breach
- Names of organizations and individuals outside your organization who were already notified of the incident
- Access to real-time IR firm analysis (an IR firm's final report is ineffective for an investigative function)
- Contact information for your organization's IR Team and/or third-party IR Firm
- Contact information for your organization's external counsel, if applicable
- Contact information for the PCI Forensic Investigator you have engaged, if applicable
- Visibility of any internal and/or external communications issued by your organization to your workforce, customers, and/or the public

Attack Scenarios

- Identify Threats (according to DBIR)
  - Social engineering
  - Basic Web Application Attacks
  - System Intrusion
  - Privilege misuse
  - Lost or stolen assets
- Mitigating
- Recovering

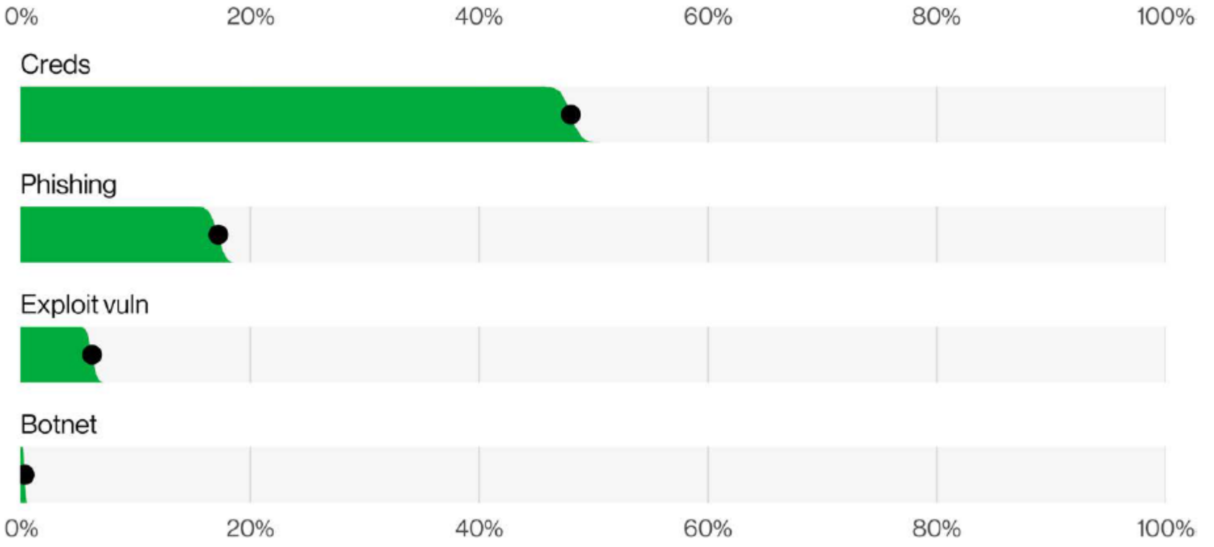
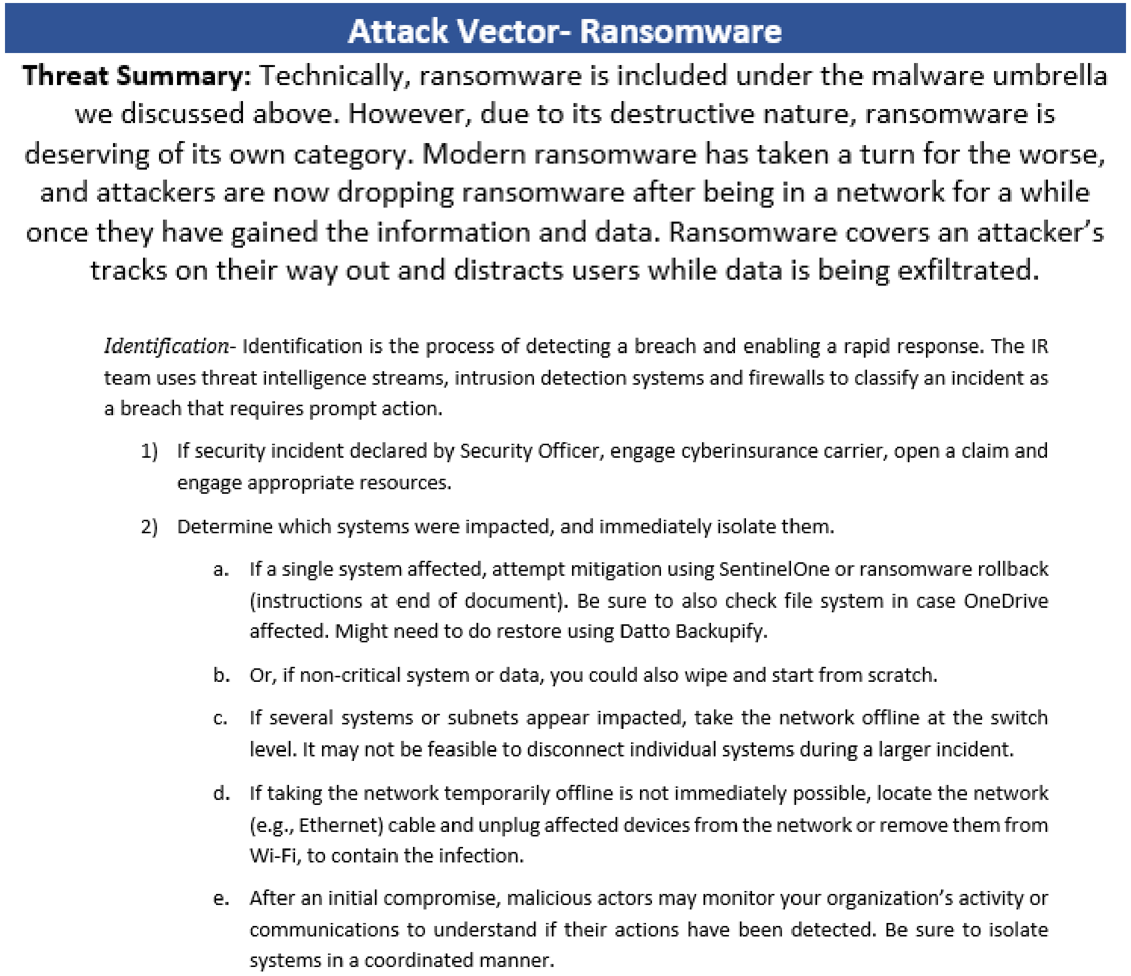


Figure 1. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

Attack Scenarios

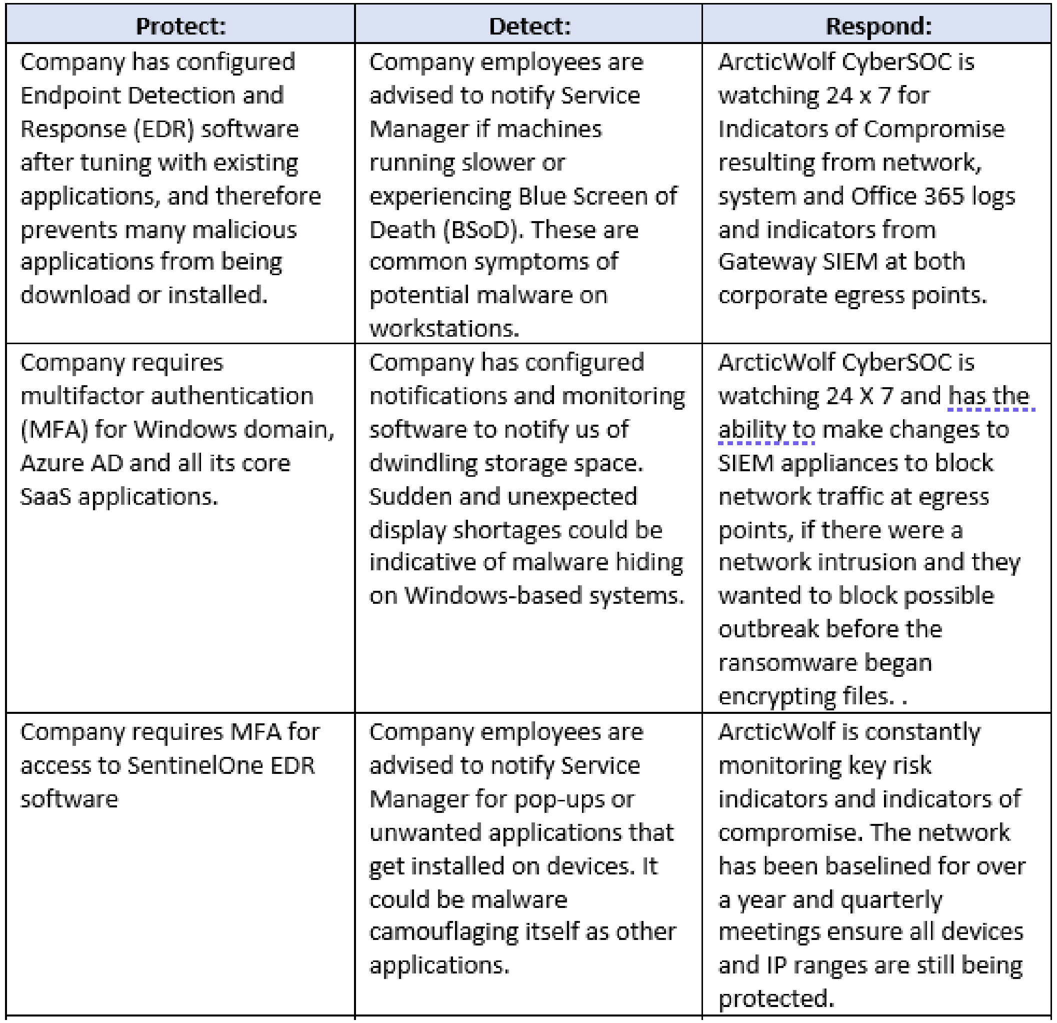


Attack Vector- Ransomware

Threat Summary: Technically, ransomware is included under the malware umbrella we discussed above. However, due to its destructive nature, ransomware is deserving of its own category. Modern ransomware has taken a turn for the worse, and attackers are now dropping ransomware after being in a network for a while once they have gained the information and data. Ransomware covers an attacker's tracks on their way out and distracts users while data is being exfiltrated.

Identification- Identification is the process of detecting a breach and enabling a rapid response. The IR team uses threat intelligence streams, intrusion detection systems and firewalls to classify an incident as a breach that requires prompt action.

1) If security incident declared by Security Officer, engage cyberinsurance carrier, open a claim and engage appropriate resources.
2) Determine which systems were impacted, and immediately isolate them.
   a. If a single system affected, attempt mitigation using SentinelOne or ransomware rollback (instructions at end of document). Be sure to also check file system in case OneDrive affected. Might need to do restore using Datto Backupify.
   b. Or, if non-critical system or data, you could also wipe and start from scratch.
   c. If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during a larger incident.
   d. If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi, to contain the infection.
   e. After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner.



Protect:	Detect:	Respond:
Company has configured Endpoint Detection and Response (EDR) software after tuning with existing applications, and therefore prevents many malicious applications from being download or installed.	Company employees are advised to notify Service Manager if machines running slower or experiencing Blue Screen of Death (BSoD). These are common symptoms of potential malware on workstations.	ArcticWolf CyberSOC is watching 24 x 7 for Indicators of Compromise resulting from network, system and Office 365 logs and indicators from Gateway SIEM at both corporate egress points.
Company requires multifactor authentication (MFA) for Windows domain, Azure AD and all its core SaaS applications.	Company has configured notifications and monitoring software to notify us of dwindling storage space. Sudden and unexpected display shortages could be indicative of malware hiding on Windows-based systems.	ArcticWolf CyberSOC is watching 24 X 7 and has the ability to make changes to SIEM appliances to block network traffic at egress points, if there were a network intrusion and they wanted to block possible outbreak before the ransomware began encrypting files. .
Company requires MFA for access to SentinelOne EDR software	Company employees are advised to notify Service Manager for pop-ups or unwanted applications that get installed on devices. It could be malware camouflaging itself as other applications.	ArcticWolf is constantly monitoring key risk indicators and indicators of compromise. The network has been baselined for over a year and quarterly meetings ensure all devices and IP ranges are still being protected.

Recovery Procedures

- Recover
  - File
  - Server
  - Service
  - Infrastructure
  - Site
- Restore
- Replace

veeAM

veeam Cloud Connect

nimble storage
a Hewlett Packard Enterprise company

datto
A Kaseya COMPANY

StorageCraft

backupify
a datto company

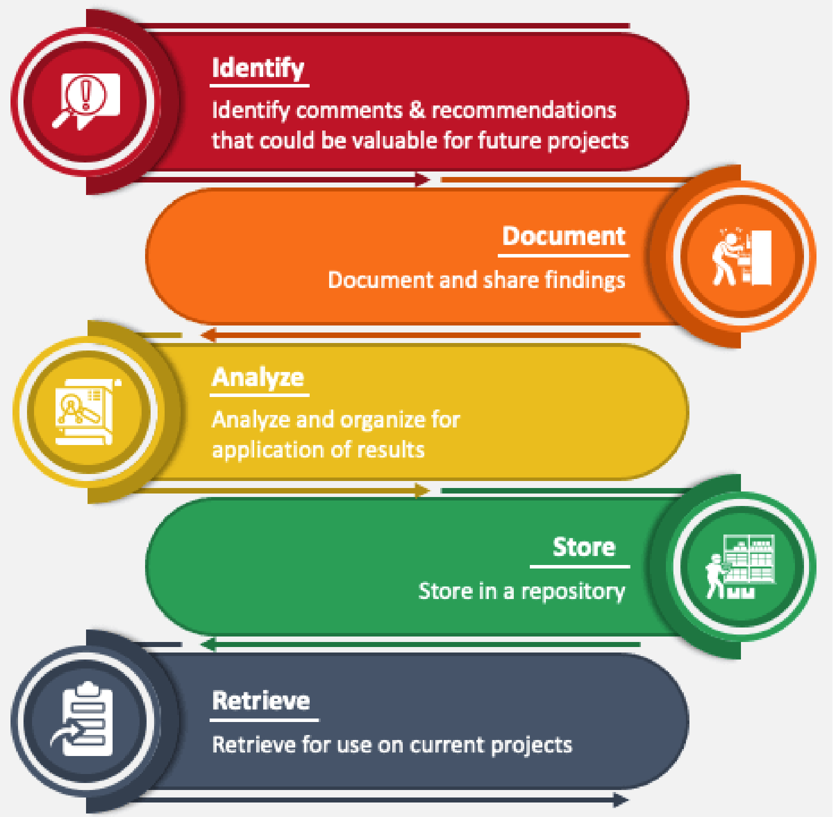
UNITRENDS
A Kaseya COMPANY

Testing

- Tabletop Exercises
- Goal- validate IRP
- Designate facilitator (focus)
- Players (active role)
- Specific Scenario(s)
- Best Practices
  - use existing plans, policies, procedures, and resources to guide
  - focus on key actions, decisions per person, problem solving
  - Keep time constraints in mind
  - low stress, no hidden agenda, no-fault
  - debrief when done, after action report

Testing

- Debrief questions
  - Was the exercise scenario realistic for your organization, processes and current security posture?
  - Did communications and processes flow as expected throughout the exercise? If not, why and where were the gaps?
  - What other plans, policies, or procedures would players implement to respond to the incident described in the exercise scenario?
  - On a scale of 1–5 (with 5 being the best), how would you rate your team on how well you handled and responded to the incident described in the exercise scenario?
  - Do you have any recommendations for improvements or areas that require follow-up?
  - Is everyone sufficiently familiar with the incident response plan established by your organization?
  - What parties and persons should be involved throughout a cyber-related incident? Are roles and responsibilities clearly defined? Are there other teams or persons in the organization who should be included?
  - What actions do all participants plan to take in order to address any outstanding issues?



Identify
Identify comments & recommendations that could be valuable for future projects

Document
Document and share findings

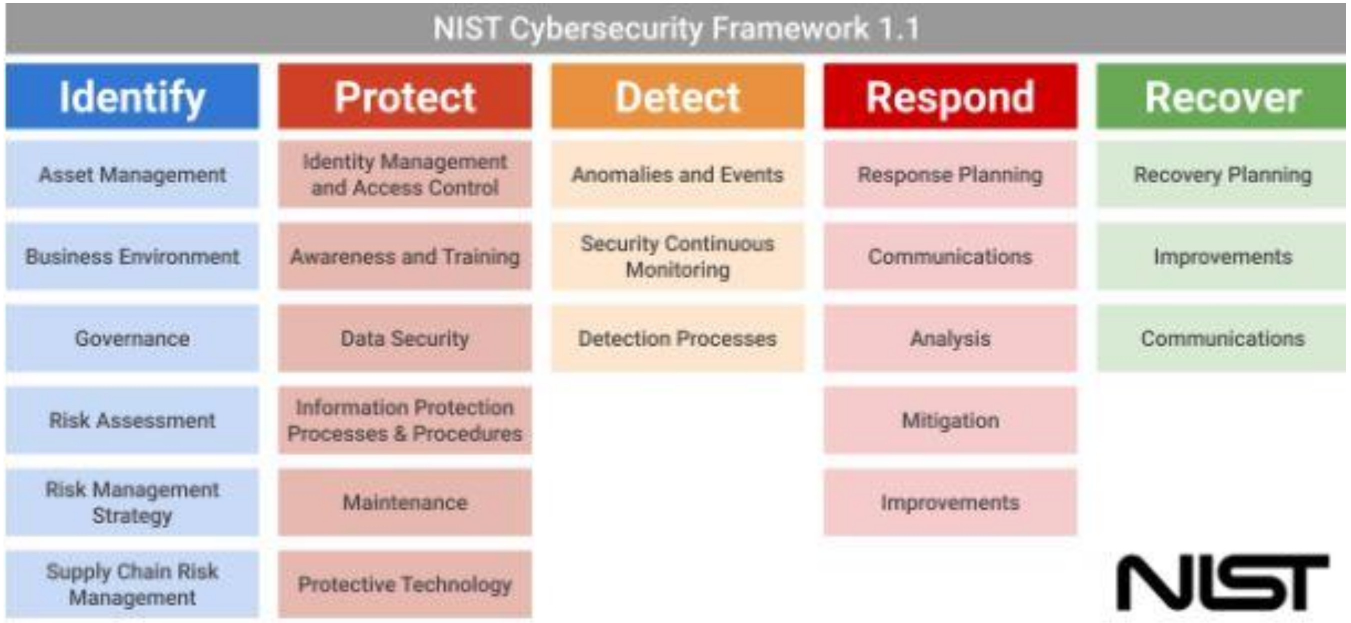
Analyze
Analyze and organize for application of results

Store
Store in a repository

Retrieve
Retrieve for use on current projects

Summary

- Get your team around you
- You probably need to do some groundwork from Identify to cover the technical aspects of the plan
- Use frameworks and resources to learn enough Incident Response
- Work out Attack Scenarios, in priority
- Organize important Recovery Procedures
- Testing your plan makes it better
- Get a better night's sleep

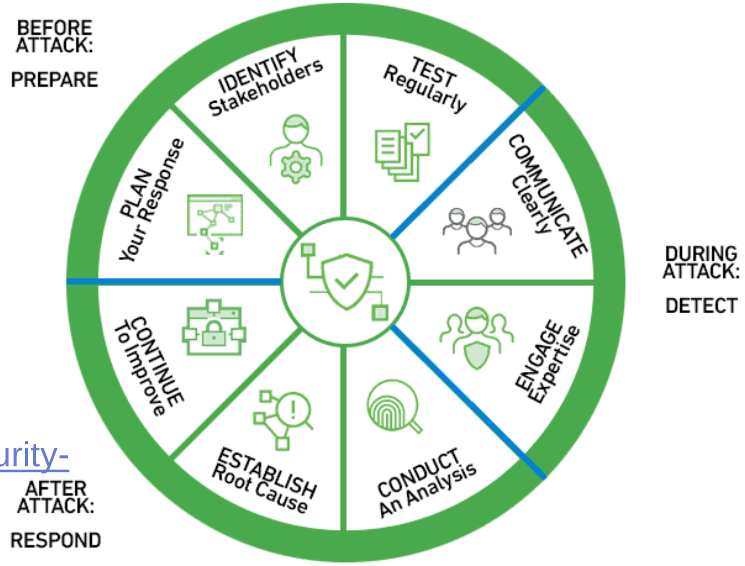


NIST Cybersecurity Framework 1.1

Identify	Protect	Detect	Respond	Recover
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

Resources

- NIST CSF- Security framework and pillars https://www.nist.gov/cyberframework
- NIST.SP.800-61r2 Computer Security Incident Handling Guide https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- Microsoft Incident Response Guide https://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-emergency-doc-digital.pdf
- IST/CIS- Blueprint for Ransomware Defense https://securityandtechnology.org/wp-content/uploads/2022/08/IST-Blueprint-for-Ransomware-Defense.pdf
- NIST.SP.800-83r1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final
- CISA Cybersecurity Incident & Vulnerability Response Playbooks https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response
- NCTCG- Cyber Security Incident Response Planning System https://www.nctcog.org/ep/resources/toolkits/cyber-security-incident-response-planning-system
- CIS- Incident Response Policy Template https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17
- SANS- The Ultimate List of SANS Cheat Sheets https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/
- State of Texas DIR- https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting
- Verizon DBIR 2022- https://www.verizon.com/business/resources/reports/2022-dbir-public-sector-snapshot.pdf



THE FULCRUM GROUP
One Technology Solution: Yours