The Human Side of IT

BUSINESS CONTINUITY + INCIDENT RESPONSE GUIDE

Tech group

A New Charter Technologies Company

IT SUPPORT | HELP DESK | NETWORK DESIGN | DISASTER RECOVERY | VOIP PHONE | CLOUD SOLUTIONS | BACKUP SOLUTIONS

The Human Side of IT

Tech group

A New Charter TECHNOLOGIES Company

BUSINESS CONTINUITY PLANNING GUIDE

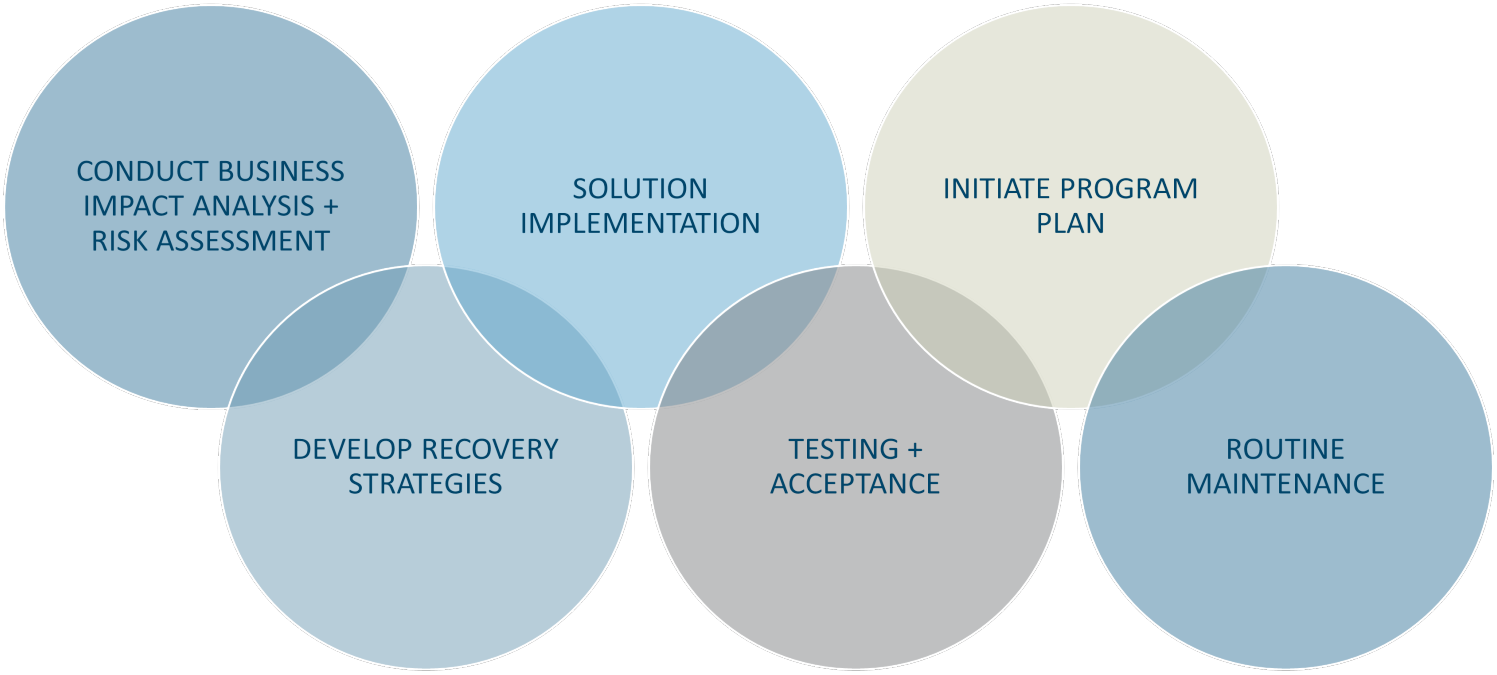
TABLE OF CONTENTS

BUSINESS CONTINUITY MANAGEMENT

Businesses cannot eliminate disasters, but proactive preparation can mitigate data loss and disruption to operations. Being prepared with a standardized, exercised, comprehensive process and procedure plan is an integral part of any Business Continuity (BC) + Disaster Recovery (DR) strategy.

The objective of a business continuity/disaster recovery plan is to ensure that you can respond to a disaster or other emergency that affects information systems and minimize the effect on the operation of the business. If you are new to recovery planning, make sure that you research the subject thoroughly before embarking on a disaster recovery project plan. Consider engaging a consultant (internal or external to your organization) to help you in your project planning effort. Disaster recovery planning is not a one and done project that once completed, you can forget about. An effective recovery plan is a live recovery plan. The plan must be maintained current and tested/exercised regularly.

The following business continuity documents and checklists are provided solely as a guide. They are only intended to give you an overview of the essential set of procedures and to be examples of conditions for you to consider for your own disaster recovery project plan. They are not, by any stretch of the imagination, the only opinions to consider when setting up a project plan to protect your organizations IT infrastructure before and after any disruption ranging from a power failure, system crash, natural disaster, or human error.



Tech group *the Human Side of IT*
A New Charter Technologies Company

BACKUP DISASTER RECOVERY STRATEGY

The accelerated digital transformation of physical being replaced by virtual is driving up the amount of digital information organizations are managing across an increasingly diverse infrastructure. An organization must be able to provide and maintain secure access to information. With major outlets reporting continued significant breach activity, organizations must take care to keep systems updated to ensure vulnerabilities in old versions aren't exposed.

Since BDR is not a primary business driver, BDR tasks often get deprioritized and put the business at risk or end up tying up time and resources that could otherwise focus on business-critical priorities. Your backup and recovery strategy plays a key role in cybersecurity. Your ability to protect and restore critical data will determine the full impact and cost of a disaster/attack. The best way to adapt your approach is with Integration and aggregation when addressing backup and disaster recovery needs.

BACKUP

Servers have incremental backups performed at various times throughout the day.

Minimize risk, maintaining multiple data backups in multiple locations.

TESTING

On site backup integrity is tested monthly by performing test restores of the data from the backup device.

Off site backup data is tested quarterly by performing a spin up of the offsite server and verify integrity of data.

Ensure you can back up and recover data for all servers across your organization and customer base.

Conduct periodic tests, external penetration and mock disaster scenarios to confirm recovery systems and practice recovery processes.

MONITORING

Backup consistency is monitored in real time throughout the day. Any issues in backups process are analyzed and remediated.

Regular Security Scorecard assessments of Operating Systems, email, backup, internet, protection + WI-FI.

DATA LOCATION

On Site backup data is encrypted in transit and at rest. The data is located on a local NAS device which is not a member of the domain and has separate unique login credentials.

Offsite data is located in a separate geographic location for geo redundancy. Offsite data is encrypted in transit and at rest.

REMEDATION

Any issues involving data recovery will first be performed at the local level. If the data at the local level is not accessible or corrupt then the offsite data will be utilized.

Third-Party Support: Leverage third-party tools as part of your BDR efforts and maintain a list of all third-party vendors you use and their contact information.

Recovery Time Objective (RTO): Establish a time frame for how quickly you want to be able to restore lost data following a disaster; this time frame can serve as a baseline for your RTO.

Establish protocols that define the roles and responsibilities of stakeholders who are involved in disaster recovery.

Tech group *the Human Side of IT*
A New Charter Technologies Company

CONTINUITY PLANNING CHECKLIST

Your organization is faced with the possibility of disruptions from a variety of sources. Your business continuity plan needs to be a top priority to allow your business to run, and people to work, exactly the same way during an emergency as they would on any other day. Business continuity plans help you to unearth your most critical risks and prepare against them by identifying and analyzing all the critical functions within your business and allow for the preparation of resource requirements.

This checklist will help you create specific strategies, and mitigation activities, to protect the critical components identified below and test the plan before it's actually needed.

INCIDENT RESPONSE TEAM

- [ ] Team coordinator
- [ ] Information security
- [ ] Systems
- [ ] Security
- [ ] Production
- [ ] Insurance
- [ ] Legal
- [ ] Public relations
- [ ] Personnel
- [ ] Audit
- [ ] Emergency response team

CRISIS COMMUNICATIONS

- [ ] Ensure strategy for internal and external crisis communication
- [ ] Ensure there are written templates and scripts for each disaster situation
- [ ] Make sure task team knows their roles in the communication plan

ISOLATE SENSITIVE INFORMATION

- [ ] Identify where sensitive information is stored/ processed
- [ ] Identify means to back up sensitive information
- [ ] Means to prioritize this information on recovery

TEST, MEASURE, AND UPDATE

- [ ] Test each disaster recovery plan for each risk situation identified
- [ ] Review any vulnerabilities or issues found during testing
- [ ] Re-evaluate your plan and fix any roadblocks

DESIGNATE A RECOVERY SITE

- [ ] Where can staff relocate if headquarters is down?
- [ ] Can staff work from home using secure VPN connections?
- [ ] Resources needed for recovery site(s)

BACK UP DATA

- [ ] Identify important data on desktops / mobile devices
- [ ] Working files
- [ ] Emails or other recorded business communications (chat/ phone calls)
- [ ] Invoices
- [ ] Tax/financial information
- [ ] Employee and customer records
- [ ] Identify backup points, replication targets
- [ ] Identify backup and disaster budget
- [ ] Protect Hard Copy Data
- [ ] Identify important documents saved as hard copies
- [ ] Contracts with suppliers or customers
- [ ] Employee information
- [ ] Tax or financial information
- [ ] Ensure digital copies of documents exist and are kept in safe places

BUSINESS CONTINUITY PLAN

- [ ] Mission-critical processes
- [ ] Mission-critical services
- [ ] Acceptable levels of service during a disaster
- [ ] Acceptable levels of production during a disaster
- [ ] Recovery Time Objectives (RTO)
- [ ] Recovery Point Objectives (RPO)
- [ ] Essential employees
- [ ] Essential sub-contractors or services
- [ ] Mission-critical technology components
- [ ] Compliance requirements governing
- [ ] Business partner essential metrics to ensure no breach of contract
- [ ] Potential threat scenarios identified
- [ ] Practical disaster recovery strategies for each scenario
- [ ] Disaster situation budget / costs of downtime and productivity

EDUCATION + TRAINING

- [ ] List contact information for all key personnel
- [ ] Ensure entire company is aware of the roles during a disaster
- [ ] Training for key personnel on the BC plan requirements
- [ ] Annual Cybersecurity Training/Seminars
- [ ] Regular vCIO Meetings + Evaluations
- [ ] Phishing Awareness Education + Training

NOTES:

*__Disclaimer:__ *Actions taken need to be tailored to your unique situation and environment. Tech Group does not take responsibility for results or outcomes.*

Tech group *the Human Side of IT*
A New Charter Technologies Company

BUSINESS IMPACT ANALYSIS CHECKLIST

Business continuity focuses on keeping business operational during a disaster, while disaster recovery focuses on restoring data access and IT infrastructure after a disaster. Analyze the impact for each potential disaster scenario.

SYSTEM FAILURE

- ☐ Identify areas of vulnerability
- ☐ People | Relationships
- ☐ Property
- ☐ Supply chain
- ☐ Production
- ☐ Information technology
- ☐ Business reputation
- ☐ Contract obligations
- ☐ Review and prioritize areas of vulnerability
- ☐ Develop mitigation strategies

NATURAL DISASTER

- ☐ Identify areas of vulnerability
- ☐ People | Relationships
- ☐ Property
- ☐ Supply chain
- ☐ Production
- ☐ Information technology
- ☐ Business reputation
- ☐ Contract obligations
- ☐ Review and prioritize areas of vulnerability
- ☐ Develop mitigation strategies

CYBER ATTACK

- ☐ Identify areas of vulnerability
- ☐ People | Relationships
- ☐ Property
- ☐ Supply chain
- ☐ Production
- ☐ Information technology
- ☐ Business reputation
- ☐ Contract obligations
- ☐ Review and prioritize areas of vulnerability
- ☐ Develop mitigation strategies

INTERNAL SABOTAGE

- ☐ Identify areas of vulnerability
- ☐ People | Relationships
- ☐ Property
- ☐ Supply chain
- ☐ Production
- ☐ Information technology
- ☐ Business reputation
- ☐ Contract obligations
- ☐ Review and prioritize areas of vulnerability
- ☐ Develop mitigation strategies

COMMUNICATION OUTAGE

- ☐ Identify areas of vulnerability
- ☐ People | Relationships
- ☐ Property
- ☐ Supply chain
- ☐ Production
- ☐ Information technology
- ☐ Business reputation
- ☐ Contract obligations
- ☐ Review and prioritize areas of vulnerability
- ☐ Develop mitigation strategies

HUMAN ERROR

- ☐ Identify areas of vulnerability
- ☐ People | Relationships
- ☐ Property
- ☐ Supply chain
- ☐ Production
- ☐ Information technology
- ☐ Business reputation
- ☐ Contract obligations
- ☐ Review and prioritize areas of vulnerability
- ☐ Develop mitigation strategies

Tech group *the Human Side of IT*
A New Charter Technologies Company

INCIDENT RESPONSE CHECKLIST

When responding to a cyber-attack, every detail is critical in protecting the business' reputation and preserving the customer's trust. The limited time to react during a breach requires that organizations have a well-thought-out and strategic approach that enables them to perform coordinated internal response efforts and swift decision making. To effectively react when notified of a breach, Tech Group believes the organization should concentrate on its ability to preserve, coordinate, and respond. The below checklist provides guidelines to handlers on the major steps that should be performed in case of cybersecurity incidents. It does not dictate the exact sequence of steps that should always be followed. The actual steps performed may vary based on the type of incident and the nature of individual incidents.

CORE RULES

Listed below are items you must have or do before you respond to a cyber incident.

CREATE AN INCIDENT RESPONSE PLAN (IR)

- ☐ Test, maintain and communicate your IR plan
- ☐ Train your team to the plan at least quarterly
- ☐ Update the plan with learnings and changes quarterly
- ☐ Communicate any and all changes to the plan
- ☐ Ensure the right people are in the right IR roles (and have backups for key roles)
- ☐ Understand attorney/client privilege
- ☐ Maintain copies of client's insurance policies
- ☐ Make IR planning and testing a requirement with executive buy-in
- ☐ Keep information about the cyber event to only those who need to know
- ☐ Don't put anything in writing unless a breach attorney instructs you to do so
- ☐ Don't use words like breach, hack, or attack prematurely. Instead, consider using the word "incident."
- ☐ Do not sacrifice forensics data in favor of restoration
- ☐ Rely on experts to help you and establish these relationships with experts now—don't just wait until an event

Tech group *the Human Side of IT*
A New Charter Technologies Company

INCIDENT RESPONSE CHECKLIST

EXECUTIVE / BUSINESS PERSPECTIVE

Responsible for critical decision making and communications

GET ON THE PHONE (NOT WITH CLIENTS YET)

- ☐ Contact cybersecurity insurance provider. They will provide you with incident response and legal resources.
- ☐ Contact legal team to ensure you have attorney/ client privilege.
- ☐ Coordinate with (insurance approved) IT provider.
- ☐ Contact law enforcement.

ORGANIZE THE TROOPS

- ☐ Have your plan ready and your IR team in place. Make any adjustments if people are not available.
- ☐ Monitor your people. These events can introduce stressful elements that people have never faced. Focus on maintaining team wellness and doing regular check-ins with everyone.
- ☐ Do not contact the bad actors until you've internally discussed the nature of the vulnerability and its overall scope. *Insurer may want to contract with a third party to handle negotiations. Ransom is often negotiable and these third parties are experienced in this area.*
- ☐ Listen to your experts.

UTILIZE YOUR TEAM

- ☐ Use your best technical staff to stop the bleeding.
- ☐ Delegate keeping the lights on to other techs.
- ☐ Have non-technical staff answering phones and responding to emails.
- ☐ Run damage control with key affected clients.

ASSESS DAMAGE

- ☐ How widespread is attack. Is it ongoing?
- ☐ Do you need to pull the plug on your own tools or temporary hot support?
- ☐ Delegate triage outreach to affected customers.
- ☐ Be aware of regulations and requirements (HIPPA, GDPR, etc.)
- ☐ Secure additional outside help/surge capacity.

GET YOUR STORY STRAIGHT

- ☐ Determine how much to share and with whom. Knowing what not to say is just as important as what you can say.
- ☐ Coordinate with teams re: communication scripts/ templates for both notifying and updating clients and responding to press inquiries.
- ☐ Ensure your messaging is approved by breach counsel. You need to ensure your internal (employee) messaging is treated with the same care and importance as external messaging.

*Disclaimer: *Any actions taken need to be tailored to your unique situation and environment. We do not take responsibility for results or outcomes.*

Tech group *the Human Side of IT*
A New Charter Technologies Company

INCIDENT RESPONSE CHECKLIST

TECHNICAL PERSPECTIVE

Responsible for containment, isolation and restoration

LOCK DOWN AFFECTED CLIENTS

- ☐ Isolate affected client endpoints by taking them off the network
- ☐ Do NOT power down or reboot any affected servers or endpoints. Disconnect them from the network to ensure memory forensics artifacts are preserved.
- ☐ Ensure backups are isolated/protected

LOCK DOWN YOUR ACCOUNTS AND TOOLS

- ☐ Audit for unusual tasks, scripts, policy changes...
- ☐ Disable user accounts associated with abnormal, malicious behavior, terminate active sessions.
- ☐ Isolate any endpoints and other accounts associated with those users.
- ☐ Minimize logging into affected systems using privileges credentials.
- ☐ DO NOT shut down affected systems
- ☐ Change all passwords.
- ☐ Ensure MFA is enabled on all accounts.
- ☐ Confirm AV is enabled and updated, run deep scan.
- ☐ If access to email is suspected... Setup email access outside of the affected domain. (*ie. Ask stakeholders to use their personal email temporarily*)
- ☐ Backup log files

NEXT STEPS AFTER ISOLATION

- ☐ Triage to determine further remediation priorities.
- ☐ Strongly consider bringing in incident response specialists.
- ☐ Gather evidence of prior network security audits, including any correspondence pertaining to previously addressed issues.

CONDUCT A REMEDIATION EVENT

- ☐ Once the incident has been properly scoped, a coordinated “remediation event” will increase the
- ☐ Chances of successfully removing the threat actor from the environment.
- ☐ Cut off access to the environment.
- ☐ Reset passwords for all (or affected) accounts.
- ☐ Identify and patch the vulnerable systems.
- ☐ Remediate malware and/or malicious remote access tooling from systems.
- ☐ Reimage or remove systems as needed.
- ☐ Revert to clean backups from before the earliest known initial threat actor access.
- ☐ Monitor closely for any indications of re-infection.

COMPLETE A POST-EVENT ANALYSIS

- ☐ Ensure your team can candidly reflect on the event—the good, the bad and the ugly.
- ☐ Review how each person performed in their role. Determine if changes need to be made.
- ☐ Modify your IR plan, if required, to reflect the lesson learned.
- ☐ Schedule an IR tabletop test for your revised plan.

*__Disclaimer:__ *Any actions taken need to be tailored to your unique situation and environment. We do not take responsibility for results or outcomes.*

Tech group *the Human Side of IT*
A New Charter Technologies Company

INCIDENT RESPONSE PLAN (TEMPLATE)

DISASTER RECOVERY PLAN			
Effective Date:		**Document Owner:**	

Revision History

Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0							

Tech group *the Human Side of IT*
A New Charter Technologies Company

INCIDENT RESPONSE PLAN TEMPLATE

PLAN OBJECTIVES

- Limit immediate incident impact to customers and business partners
- Recover from the incident
- Determine how the incident occurred
- Find out how to avoid further exploitation of the same vulnerability
- Avoid escalation and further incidents
- Assess the impact and damage in terms of financial impact and loss of image
- Update company policies, procedures, standards, and guidelines as needed; and
- Determine who initiated the incident for possible criminal and/or civil prosecution.

MALICIOUS ACTONS	POSSIBLE INDICATIONS OF AN INCIDENT
Denial of Service (DoS) Examples	**You might be experiencing a DoS if you see…**
Network-based DoS against a particular host	• User reports of system unavailability • Unexplained connection losses • Network intrusion detection alerts • Host intrusion detection alerts (until the host is overwhelmed) • Increased network bandwidth utilization • Large number of connections to a single host • Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) • Firewall and router log entries • Packets with unusual source addresses
Network-based DoS against a network	• User reports of system and network unavailability • Unexplained connection losses • Network intrusion detection alerts • Increased network bandwidth utilization • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) • Firewall and router log entries • Packets with unusual source addresses • Packets with nonexistent destination addresses
DoS against the operating system of a particular host	• User reports of system and application unavailability • Network and host intrusion detection alerts • Operating system log entries • Packets with unusual source addresses
DoS against an application on a particular host	• User reports of application unavailability • Network and host intrusion detection alerts • Application log entries • Packets with unusual source addresses

MALICIOUS ACTONS	POSSIBLE INDICATIONS OF AN INCIDENT
Malicious Software (Malware) Examples	**You might be experiencing a DoS if you see…**
A virus that spreads through email infects a host.	• Antivirus software alerts of infected files • Sudden increase in the number of emails being sent and received • Changes to templates for word processing documents, spreadsheets, etc. • Deleted, corrupted, or inaccessible files • Unusual items on the screen, such as odd messages and graphics • Programs start slowly, run slowly, or do not run at all • System instability and crashes
A worm that spreads through a vulnerable service infects a host.	• Antivirus software alerts of infected files • Port scans and failed connection attempts targeted at the vulnerable service (e.g.: open Windows shares, HTTP) • Increased network usage • Programs start slowly, run slowly, or do not run at all • System instability and crashes
A Trojan horse is installed and running on a host.	• Antivirus software alerts of Trojan horse versions of files • Network intrusion detection alerts of Trojan horse client-server communications • Firewall and router log entries for Trojan horse client-server communications • Network connections between the host and unknown remote systems • Unusual and unexpected ports open • Unknown processes running • High amounts of network traffic generated by the host, particularly if directed at external host(s) • Programs start slowly, run slowly, or do not run at all • System instability and crashes
Malicious mobile code on a website is used to infect a host with a virus, worm, or Trojan horse.	• Indications listed above for the pertinent type of malicious code • Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes
Malicious mobile code on a Web site exploits vulnerabilities on a host.	• Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes • Sudden increase in the number of emails being sent and received • Network connections between the host and unknown remote systems
A user receives a virus hoax message.	• Original source of the message is not an authoritative computer security group, but a government agency or an important official person • No links to outside sources • Tone and terminology attempt to invoke panic or a sense of urgency • Urges recipients to delete certain files and forward the message to others

MALICIOUS ACTONS	POSSIBLE INDICATIONS OF AN INCIDENT
Unauthorized Access Examples	**You might be experiencing a DoS if you see…**

Root compromise of a host	• Existence of unauthorized security-related tools or exploits
	• Unusual traffic to and from the host (e.g.: attacker may use the host to attack other systems)
	• System configuration changes, including:
	  ○ Process/service modifications or additions
	  ○ Unexpected open ports
	  ○ System status changes (restarts, shutdowns)
	  ○ Changes to log and audit policies and data
	  ○ Network interface card set to promiscuous mode (packet sniffing)
	  ○ New administrative-level user account or group
	• Modifications of critical files, timestamps, and privileges, including executable programs, OS kernels, system libraries, and configuration and data files
	• Unexplained account usage (e.g.: idle account in use, account in use from multiple locations at once, unexpected commands from a particular user, large number of locked-out accounts)
	• Significant changes in expected resource usage (e.g.: CPU, network activity, full logs, or file systems)
	• User reports of system unavailability
	• Network and host intrusion detection alerts
	• New files or directories with unusual names (e.g.: binary characters, leading spaces, leading dots)
	• Highly unusual operating system and application log messages
	• Attacker contacts the organization to say that he or she has compromised a host

Unauthorized data modification (e.g.: Web server defacement)	• Network and host intrusion detection alerts • Increased resource utilization • User reports of the data modification (e.g.: defaced Web site) • Modifications to critical files (e.g.: Web pages) • New files or directories with unusual names (e.g.: binary characters, leading spaces, leading dots) • Significant changes in expected resource usage (e.g.: CPU, network activity, full logs or file systems)
Unauthorized usage of standard user account	• Access attempts to critical files (e.g.: password files) • Unexplained account usage (e.g.: idle account in use, account for use from multiple locations at once, commands that are unexpected from a particular user, large number of locked-out accounts) • Web proxy log entries showing the download of attacker tools
Physical intruder	• User reports of network or system unavailability • System status changes (restarts, shutdowns) • Hardware is completely or partially missing (i.e.: a system was opened, and a particular component removed) • Unauthorized new hardware (e.g.: attacker connects a packet sniffing laptop to a network or a modem to a host)
Unauthorized data access (e.g.: database of customer information, password files)	• Intrusion detection alerts of attempts to gain access to the data through FTP, HTTP, and other protocols • Host-recorded access attempts to critical files

MALICIOUS ACTONS	POSSIBLE INDICATIONS OF AN INCIDENT
Inappropriate Usage Examples	**You might be experiencing a DoS if you see…**

Unauthorized service usage (e.g.: Web server, file sharing, music sharing)	• Network intrusion detection and network behavior analysis software alerts
	• Unusual traffic to and from the host
	• New process/software installed and running on a host
	  ○ Password cracking tools
	  ○ Unauthorized website running
	  ○ File transfer software
	  ○ Peer-to-Peer (P2P) sharing software running
	• New files or directories with unusual names (e.g.: “warez” server style names)
	• Increased resource utilization (e.g.: CPU, file storage, network activity)
	• User reports
	• Application log entries (e.g.: Web proxies, FTP servers, email servers)

Access to inappropriate materials (e.g.: downloading pornography, sending spam)	• Network intrusion detection alerts • Eyewitness reports or complaints to management, HR, or ethics ○ Pornographic or explicit content displayed • Application log entries (e.g.: Web proxies, FTP servers, email servers) • Inappropriate files on workstations, servers, or removable media

Attack against internal party	• Network intrusion detection alerts
	• Inside party reports (e.g.: management, HR, or ethics)
	  ○ Harassing email or text messages sent to internal users
	  ○ Pornographic or explicit content sent to internal users
	• Network, host, and application log entries

Attack against external party	• Network intrusion detection alerts
	• Outside party reports
	  ○ Harassing email or text messages sent to external users
	  ○ Pornographic or explicit content sent to external users
	  ○ External attack traffic traced back to the company
	• Network, host, and application log entries

COMMON EFFECTS OF ATTACKS

There are at least four primary effects of attacks that affect Information Security:

DENIAL OF SERVICE

Any action that causes all or part of the network's service to be stopped entirely, interrupted, or degraded sufficiently to impact operations. Examples of denial of service include network jamming, introducing fraudulent packets, and system crashes and/or poor system performance, in which people are unable to effectively use computing resources.

LOSS / ALTERATION OF DATA OR PROGRAMS.

An example of loss or alteration of data or programs would be an attacker who penetrates a system, then modifies an Operating System-level program/configuration file (e.g.: audit) so that the intrusion will not be detected.

COMPROMISE OF DATA.

One of the major dangers of a computer security incident is that information may be compromised. The release of classified information to people without the proper clearance or formal authorization jeopardizes our nation's security. Efficient incident handling minimizes this danger.

LOSS OF TRUST IN COMPUTING SYSTEMS.

Users may lose trust in computing systems and become hesitant to use one that has a high frequency of incidents or even a high frequency of events that cause the user to distrust availability or integrity.

INCIDENT RESPONSE STAGES

There are generally six (6) stages of incident response:

PREPARATION

The most important facilities to a response plan are to know how to use it once it is in place. Knowing how to respond to an incident before it occurs can save valuable time and effort in the long run.

IDENTIFICATION.

Identify whether or not an incident has occurred. If one has occurred, the Incident Response Team can take the appropriate actions. Identification may come from Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), File Integrity Monitoring Systems (FIMS), or manual observance of an incident

CONTAINMENT

Involves limiting the scope and magnitude of an incident. Because so many incidents observed currently involve malicious code, incidents can spread rapidly. This can cause the destruction and loss of data. As soon as an incident is recognized, the Incident Response Team must immediately begin working on containment.

ERADICATION

Removing the cause of the incident can be a difficult process. It can involve virus removal, removing user permissions, and/or dismissing employees.

RECOVERY.

Restoring a system to its normal business status is essential. Once a restore has been performed, it is also important to verify that the restore operation was successful and that systems are back to its normal condition.

FOLLOW-UP.

Some incidents require considerable time and effort. It is common that once the incident appears to be contained and remedied; there is little interest in devoting any more effort to the incident. Performing follow-up activity is, however, one of the most critical activities in the response procedure. This follow-up can support any efforts to prosecute those who have broken the law. This includes changing any policies that may need to be narrowed down or be changed altogether.

SECURITY SOFTWARE ALERTS

TYPE	SOURCE	DESCRIPTION
Computer Security Software Alerts		
Technical	Network-based, host-based, and wireless IDS	Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) products are designed to identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use a set of attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces false positives—alerts that indicate malicious activity is occurring, when in fact, there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.
Technical	Antivirus, antispyware, and antispam software	Antivirus and antispyware software are designed to detect various forms of malicious code and prevent them from infecting hosts. When antivirus or antispyware software detects malicious code, it typically generates alerts. Current antivirus and antispyware products are effective at detecting and eradicating or isolating malicious code if their signatures are kept up to date.
Technical	File integrity checking software	Incidents may cause changes to important files; file integrity checking software can detect such changes. It works by using a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
Technical	3rd Party Monitoring service	Some organizations pay a third party to monitor their publicly accessible services, such as Web, Domain Name System (DNS) and FTP servers. The third party automatically attempts to access each service every x minutes. If the service cannot be accessed, the third party alerts the organization using the methods specified by the organization, such as phone calls, pages, and emails.
Logs		
Technical	Operating system, security, and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs. Logs can provide a wealth of information, such as which accounts were accessed and what actions were performed.
Technical	Network device logs	Logs from network devices such as firewalls and routers are not typically used as a primary source of precursors or indications. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity.
Publicly Available Information		
Human	Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in the detection and analysis of new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities. Several organizations, such as US-CERT, CERT®/CC, IAIP, and the Department of Energy's Computer Incident Advisory Capability (CIAC), periodically provide threat update information through briefings, Web postings, and mailing lists.
Human	Information on incidents at other organizations	Reports of incidents that have occurred at other organizations can provide a wealth of information. There are Web sites and mailing lists where incident response teams and security professionals can share information regarding reconnaissance and attacks that they have seen. In addition, some organizations acquire, consolidate, and analyze logs and intrusion detection alerts from many other organizations.

TYPE	SOURCE	DESCRIPTION
People		
Human	Internal Users	Users, system administrators, network administrators, security staff, and others from within the organization may report signs of incidents. It is important to validate all such reports. Not only do users generally lack the knowledge to determine if an incident is occurring, but also even the best-trained technical experts make mistakes. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.
Human	Other Organizations	Although few reports of incidents will originate from people at other organizations, they should be taken seriously. A classic example is an attacker who identifies a serious vulnerability in a system and either informs the organization directly or publicly announces the issue. Another possibility is that the organization might be contacted by an external party claiming someone at the organization is attacking it. External users may also report other indications, such as a defaced Web page or an unavailable service. Other incident response teams also may report incidents.

INCIDENT CATEGORIES

An incident will be categorized as one of ten severity levels. These severity levels are based on the impact to the company and can be expressed in terms of financial impact, impact to operations, impact to sales, or impact to the company's image.

CAT	SEVERITY	SITUATION	DETAILS
0	Training	**Exercise (e.g. Network Defense Testing)**	**Description:** Used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.
			Response Action: Depends on the type of exercise.
			Response Time: Exercise Dependent
			Recovery Actions: There are no recovery procedures required for this event.
1	Criminal	**Illegal Content**	**Description:** Used to respond to any suspected incidents involving either: • The possession or transmission of child pornography; or • Possible terrorist-related activities
			Response Action: Stop the investigation immediately. The incident handler must cease work and call the local office for the FBI and follow the FBI's response instructions
			Response Time: Within 1 hour of event identification
			Recovery Actions: There are no recovery procedures required for this event.
2	Serious	**Successful Host Compromise (Privileged-level access)**	**Description:** This is a root or administrator-level compromise of a system. A successful event of this nature means the intruder has total control over the host and access to any and all data stored on it or on systems that trust this host.
			Response Action: The system must be disconnected from the network. It should NOT be turned off. No action should be taken to investigate this incident of change anything on the system unless directed to do so by IT Support.
			Response Time: Within 1 hour of event identification
			Recovery Actions: Do not start recovery procedures until directed to do so by IT Support. Normal recovery procedures from an event of this category: rebuilding the system from original media, installing required patches, and scanning for vulnerabilities before reattaching to the network. Notify IT Support to arrange for a verification scan to be conducted.

INCIDENT CATEGORIES Cont.

CAT	SEVERITY	SITUATION	DETAILS
3	Serious	**Malicious Software (servers)**	**Description:** Any software code intentionally created or introduced into a server-class system for the distinct purpose of causing hard or loss to the computer system, its data, or other resources. Examples are spyware, adware, viruses, Trojans, worms, etc. **Response Action:** The system must be disconnected from the network. It should NOT be turned off. No action should be taken to investigate this incident of change anything on the system unless directed to do so by IT Support. **Response Time:** Within 1 hour of event identification **Recovery Actions:** Recovery procedures until directed to do so by IT Support. Normal recovery procedures from an event of this category are rebuilding the system from original media, installing all required patches, and scanning for vulnerabilities before reattaching to the network. Notify IT Support to arrange for a verification scan to be conducted.
4	Serious	**Malicious Software (workstations)**	**Description:** Any software code intentionally created or introduced into a workstation-class system for the distinct purpose of causing hard or loss to the computer system, its data, or other resources. Examples are spyware, adware, viruses, Trojans, worms, etc. **Response Action:** The system must be disconnected from the network. It should NOT be turned off. IT Support will respond and follow company-approved procedures to remediate the malware infection. **Response Time:** Within 1 hour of event identification **Recovery Actions:** Normal recovery procedures from an event of this category are rebuilding the system from original media, installing all required patches, and scanning for vulnerabilities before reattaching to the network. Notify IT Support to arrange for a verification scan to be conducted.
5	Serious	**Denial of Service (DoS) Attack**	**Description:** A successful event of this nature means the intruder has successfully denied access to either the entire network, portion of the network or to critical systems or data. **Response Action:** Determine the cause, if at all possible. Contact IT Support for assistance in determining the source of the attack and removing the threat. Take no further action unless directed to do so by IT Support. **Response Time:** Within 1 business day **Recovery Actions:** Review logs and configurations to determine if there is anything that can be done to prevent further occurrences of this type of the event and/or the cause of the current event
6	Serious	**Unauthorized Scan (internal network)**	**Description:** Any automated probe attacks (e.g. Nessus, Nmap, etc.) **Response Action:** Contact IT Support for assistance in determining if the scan is unauthorized. **Response Time:** Within 1 business day **Recovery Actions:** Review system event logs and/or network logs to determine if any systems responded to the probe or scan and what information may have been obtained by the unauthorized scanner.

INCIDENT CATEGORIES Cont.

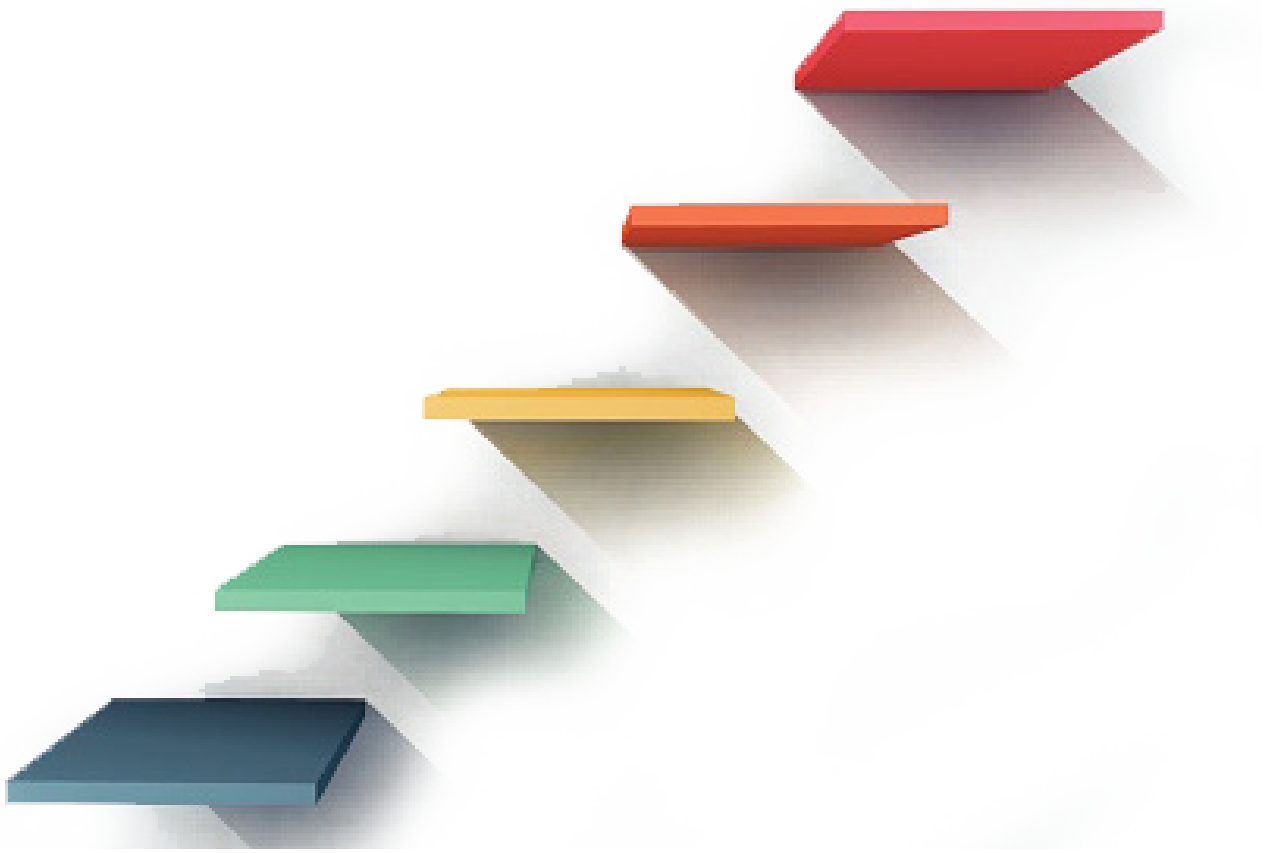
CAT	SEVERITY	SITUATION	DETAILS
7	Significant	Successful Host Compromise (user-level access)	**Description:** This is a user-level compromise. A successful event of this nature means the intruder has access to data, applications, and systems which the users is allowed to access.
			Response Action: The system must be disconnected from the network. It should NOT be turned off. No action should be taken to investigate this incident of change anything on the system unless directed to do so by IT Support.
			Response Time: Within 1 business day
			Recovery Actions: Do not start recovery procedures until directed to do so by IT Support. Normal recovery procedures from an event of this category are rebuilding the system from original media, installing all required patches, and scanning for vulnerabilities before reattaching to the network.
8	Significant	Attempted Access (unsuccessful)	**Description:** An unsuccessful attempt to access or compromise an information system. An event of this nature means the intruder attempted a known exploit or attempted to log into an information system but was not successful in compromising it or in logging in.
			Response Action: No response is necessary. Report the event to IT Support and include as much data as possible about the intruder and the attempted compromise or intrusion. Take no further action unless directed to do so by IT Support.
			Response Time: Within 1 business day
			Recovery Actions: There are no recovery procedures required for this event.
9	Significant	Poor Security Practice	**Description:** security practices are root login using Telnet, FTP or HTTP; bad passwords; not using secure protocols to transfer sensitive data; downloading unauthorized software; peer-to-peer (P2P) software, etc.
			Response Action: The response depends on the event. The response ranges from disconnection from the network to a system rebuild, to no action required. An incident report should be sent to the department to follow appropriate actions (e.g.: verbal or written counseling).
			Response Time: Within 1 business day
			Recovery Actions: The recovery depends on the type of event.
10	Significant	Unknown	**Description:** If the threat is unclear, use this category until the threat or situation is investigated, and a final determination has been made.
			Response Action: Reassign to the proper category when a final determination is made.
			Response Time: Within 4 hours of event identification
			Recovery Actions: Recovery is determined after the final determination and event category is determined

ESCALATION LEVEL CONSIDERATIONS

Incident Response management must consider several characteristics of the incident before escalating the response to a higher level. These considerations include:

- Legal requirements for breach notification?
- How widespread is the incident?
- What is the impact to business operations?
- How difficult is it to contain the incident?
- How fast is the incident propagating?
- What is the estimated financial impact of CLIENT_NAME?
- Will this negatively affect CLIENT_NAME 's image?

.



INCIDENT RESPONSE PROCESS

The Incident Response Process is an escalation process whereas the impact of the incident becomes more significant or widespread, the escalation level increases bringing more resources to bear on the problem. At each escalation level, team members who will be needed at the next higher level of escalation are alerted to the incident so that they will be ready to respond if and when they are needed.

DETECTION AND ANALYSIS PHASE

STEP		RESPONSIBLE ENTITY	INCIDENT RESPONSE PLAN (IRP) ACTIONS	✓
1	**1.0**	**Anyone**	**Determine If an Incident Occurred**	
	1.1	**Anyone**	Analyze the precursors and indications.	
	1.2	**Anyone**	Look for correlating information.	
	1.3	**Anyone**	Perform research (e.g.: search engines, vendor knowledge base, peer review, etc.)	
	1.4	**Anyone**	As soon as the incident handler believes an incident has occurred, he/she must begin documenting the incident and gathering evidence.	
2	**2.0**	**Anyone**	**Notify IT Support**	
	2.1	**Anyone**	The incident handler contacts IT Support and provides available documentation and evidence.	
	2.2	**IT Support**	IT Support classifies the incident.	
	2.3	**IT Support**	If the IT Support categorizes the event as a full investigation, the IT Support technician should create a case file.	
	2.4	**IT Support**	IT Support on-call analyst consolidates documentation and evidence and, if applicable, stores the documentation in the case folder for the incident.	
3	**3.0**	**IT Support**	**Incident Prioritization**	
	3.1	**IT Support**	IT Support prioritizes handling the incident based on the business impact.	
	3.2	**IT Support**	IT Support will identify which IT resources have been affected and forecast which resources will be affected.	
	3.3	**IT Support**	IT Support will estimate the current and potential technical effect of the incident.	
4	**4.0**	**IT Support**	**Incident Notification**	
	4.1	**IT Support**	IT Support will contact affected asset owners and business units, alerting them to the situation.	
5	**5.0**	**Multiple Entities**	**Incident Escalation (If Required)**	
	5.1	**IT Support**	If the incident is believed to be significant, the IT Support technician or asset owner is responsible for notifying management for escalation.	
	5.2	**Management**	Management is responsible for coordinating further incident escalation steps, as required.	

CONTAINMENT, ERADICATION, AND RECOVERY PHASE

STEP		RESPONSIBLE ENTITY	INCIDENT RESPONSE PLAN (IRP) ACTIONS	✓
6	**6.0**	**IT Support**	**Secure, Document, Acquire, Preserve & Analyze Evidence (If Required)**	
	6.1	**IT Support**	IT Support will follow its Standard Operating Procedures (SOP) for evidence seizure and analysis.	
7	**7.0**	**Multiple Entities**	**Contain the Incident**	
	7.1	**IT Support**	IT Support will work with affected asset custodians and business units to determine a containment strategy.	
	7.2	**Multiple Entities**	Incident handlers will implement steps to contain the incident.	
8	**8.0**	**Multiple Entities**	**Eradicate the Incident**	
	8.1	**Multiple Entities**	Identify and mitigate all vulnerabilities that were exploited.	
	8.2	**Multiple Entities**	Remove malicious code, inappropriate materials, and other components.	
9	**9.0**	**Multiple Entities**	**Recover From the Incident**	
	9.1	**Multiple Entities**	Return affected systems to an operationally ready state.	
	9.2	**Multiple Entities**	Confirm that the affected systems are functioning normally.	
	9.3	**Multiple Entities**	If necessary, implement additional monitoring to look for future related activity.	

POST-INCIDENT ACTIVITY PHASE

STEP		RESPONSIBLE ENTITY	INCIDENT RESPONSE PLAN (IRP) ACTIONS	✓
Post-Incident Activity Phase				
10	10.0	**IT Support**	**Follow-Up Report**	
	10.1	**IT Support**	IT Support will create a follow-up report and distribute it appropriately.	
11	11.0	**Multiple Entities**	**After Action Review (AAR)**	
	11.1	**Multiple Entities**	Hold an After-Action Review (AAR) / "lessons learned" meeting involving all key players.	
	11.2	**Multiple Entities**	Update any changes needed to the Incident Response Plan (IRP) or other policy/procedure/standard.	

INCIDENT RESPONSE TEAM (24X7)

To adequately respond to an intrusion or incident, predetermined teams should be formed to react to predetermined incident characteristics. As the situation develops and the impact becomes more significant, the various teams may be called to contribute.

INCIDENT RESPONSE TEAM ROLES (24x7 Key Personnel)	ROLE DESCRIPTION
Name	**Incident Response Coordinator.** Individual responsible for conducting and coordinating the Incident Response Plan (IRP).
Name	**Technical Support Team Lead.** Individual responsible for providing assistance to IT support, which could include support personnel, outside contractors, or individual users.
Name	**Management Team Lead.** Management representative responsible for interfacing with other managers/executives in areas, such as Legal, Human Resources, or other specialties, as required.

INCIDENT RESPONSE TEAM CAPABILITIES

INCIDENT RESPONSE COORDINATOR:

- Receive and track all reported potential threats.
- Escalate Incident Response if the threat manifests itself.
- Determine relevant membership of the Technical Support Team.
- Alert applicable support organizations of the potential threat and any defensive action required.
- Alert management of the potential threat.
- Start a chronological log of events.
- Receive status from IT Support and report to management on a regular basis.

TECHNICAL SUPPORT TEAM:

- Monitor all applicable sources for alerts or notification of a threat.
- Determine initial defensive actions required.
- Notify the Incident Response Coordinator.
- Determine the best course of action for the containment of the incident and eradication of the threat.
- Report actions taken and status to the Incident Response Coordinator.
- Continue to monitor all sources for alerts looking for more information or actions to take to eliminate the threat.
- Continue reporting status/actions taken to the Incident Response Coordinator for a chronological log of events.
- Monitor effectiveness of actions taken and modify them as necessary.

MANAGEMENT TEAM:

- Assume responsibility for directing activities, in regard to the incident.
- Actively participate in Incident Response operations, based on the effects to business operations.
- Determine whether escalation appropriate.
- Determine when the risk has been mitigated to an acceptable level.
- Contact local authorities, if deemed appropriate.
- Initial breach notification procedures, if applicable.
- Ensure that all needed information is being collected to support legal action or financial restitution.

INCIDENT NOTIFICATION REQUIREMENTS

CLIENT_NAME must perform an annual review of notification requirements to determine who must be contacted and the timeline for notification following the identification of a data breach:

- Applicable state breach notification regulatory requirements
- Applicable Federal breach notification regulatory requirements
- Contractual obligations for breach notification

POST INCIDENT REQUIREMENTS

Following an incident, the Incident Response Coordinator should work with the Technical Support Team to prepare a report for management to include:

- Estimate of damage and impact.
- Action taken during the incident (not technical detail).
- Follow-on efforts needed to eliminate or mitigate the vulnerability.
- Policies or procedures that require updating.
- Efforts taken to minimize liabilities or negative exposure.
- Provide the chronological log and any system audit logs requested by the Management Team.
- Document lessons learned and modify the Incident Response Plan (IRP) accordingly.
- Recommend disciplinary action in the case that the incident was from an internal source.

Tech group *the Human Side of IT*
A New Charter Technologies Company

CYBER LIABILITY

A vital step in safeguarding your business, protecting your customers' information and your livelihood, is by analyzing your potential risks to put measures in place to protect and avoid attacks. The following questions are commonly asked by insurance providers to help you determine where your vulnerabilities may be. If your insurance company has additional questions, please reach out and we will provide more explanation as needed.

INFORMATION AND NETWORK SECURITY CONTROLS	
Do you use a cloud provider to store data or host applications?	
Do you use Multi-Factor Authentication (MFA) to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud)?	
Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? [If "No", are compensating controls in place: Segregation of servers that store sensitive/confidential information or Access control with role-based assignments]?	
Do you use an endpoint protection (EPP) product across your enterprise?	
Do you use an endpoint detection and response (EDR) product across your enterprise?	
Do you use MFA to protect privileged user accounts?	
Is a hardened baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices? [Yes, No, Partial]	
What % of the enterprise is covered by your scheduled vulnerability scans?	
In what time frame do you install critical and high severity patches across your enterprise? [within 2 weeks, 1 mo., 2 mo., Ad Hoc]	
If you have any end of life or end of support software, is it segregated from the rest of the network? [Yes, No, Partial, N/A]	
Have you configured host-based and network firewalls to disallow inbound connections by default? [Yes, No, Partial]	
Do you use a protective DNS service (e.g. Quad9, Open DNS or the public sector PDNS)?	
Do you use an endpoint application isolation and containment technology?	
Do your users have local admin rights on their laptop / desktop?	
Can users run MS Office Macro enabled documents on their system by default? [Yes, No, Partial]	
Do you provide your users with a password manager software?	
Do you manage privileged accounts using tooling? [Yes, No, Partial]	
Do you have a security operations center established, either in-house or outsourced? [Yes-24x7, Yes-working hours, No]	

RANSOMWARE CONTROLS	
Pre-screen e-mails for potentially malicious attachments and links?	
Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if they are malicious prior to delivery to the end-user?	
Can your users access email through a web application or a non-corporate device?	
Do you enforce MFA for users accessing email through a web application or a non-corporate device?	
Do you allow remote access to your network?	
Do you use MFA to secure all remote access to your network, including any remote desktop protocol (RDP) connections?	
Do you use a next-generation anti-virus (NGAV) product to protect all endpoints across your enterprise?	
Do you use MFA to protect access to privileged user accounts?	
Do you use a data backup solution [Daily, Weekly, Monthly]?	
Do you use a Cloud syncing service for backups? (E.g. Dropbox, OneDrive, SharePoint, Google Drive)	
Estimated amount of time it will take to restore essential functions in the event of a widespread malware or ransomware attack within your network?	
Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months? [Yes, No, Partial]	
Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware? [Yes, No, Partial]	
Backups are secured with different access credentials from other administrator credentials?	
Are your backups encrypted?	
Backups are kept separate from your network (offline/air-gapped), or in a cloud service designed for this purpose. [Yes-fully offline, Yes-cloud service, Yes-partially offline, No]	

Tech group *the Human Side of IT*
A New Charter Technologies Company

CYBER LIABILITY cont.

PHISHING CONTROLS	
Do any of the following employees at your company complete social engineering training? (No, Yes: All, C-Suite, Financial Responsibility, Other select)	
If "Yes" to question A. or B. above, does your social engineering training include phishing simulation?	

EMAIL SECURITY	
Provide a quarantine service to your users?	
Strictly enforce Sender Policy Framework (SPF) on incoming e-mails?	
How often is phishing training conducted to all staff (Monthly, Quarterly, Annually)?	
If Yes: Do you use the o365 Advanced Threat Protection add-on?	

OTHER SECURITY PREVENTATIVE MEASURES

Note any additional steps your organization takes to detect and prevent ransomware attacks (e.g. segmentation of your network, additional software tools, external security services, etc.).

A FEW TYPICAL NON IT QUESTIONS	
Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form?	
Does your organization send and/or receive wire transfers?	
If "Yes", does your wire transfer authorization process include the following:	
A wire request documentation form?	
A protocol for obtaining proper written authorization for wire transfers?	
A separation of authority protocol?	
A protocol for confirming all payment or funds transfer instructions/requests from a new vendor, client or customer via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the payment or funds transfer instruction/request was received?	
A protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information or mailing addresses) via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the change request was received?	

Tech group *the Human Side of IT*
A New Charter Technologies Company

CYBER LIABILITY

SAMPLE

The following questions are commonly asked by insurance providers to help you determine where your vulnerabilities may be. The answers we have provided below are considered "best practice" for a typical Tech Group client. Your own answers may differ based on your individual organizational requirements and management decisions.

INFORMATION AND NETWORK SECURITY CONTROLS	
Do you use a cloud provider to store data or host applications?	YES
Do you use Multi-Factor Authentication (MFA) to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud)?	YES
Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? [If "No", are compensating controls in place: Segregation of servers that store sensitive/confidential information or Access control with role-based assignments]?	No or Sensitive data is store with-in applica-tion that is encrypted
Do you use an endpoint protection (EPP) product across your enterprise?	YES
Do you use an endpoint detection and response (EDR) product across your enterprise?	YES
Do you use MFA to protect privileged user accounts?	In Process
Is a hardened baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices? [Yes, No, Partial]	Partial
What % of the enterprise is covered by your scheduled vulnerability scans?	100%
In what time frame do you install critical and high severity patches across your enterprise? [within 2 weeks, 1 mo., 2 mo., Ad Hoc]	within 2 weeks
If you have any end of life or end of support software, is it segregated from the rest of the network? [Yes, No, Partial, N/A]	Per Client
Have you configured host-based and network firewalls to disallow inbound connections by default? [Yes, No, Partial]	YES
Do you use a protective DNS service (e.g. Quad9, Open DNS or the public sector PDNS)?	YES
Do you use an endpoint application isolation and containment technology?	YES
Do your users have local admin rights on their laptop / desktop?	YES
Can users run MS Office Macro enabled documents on their system by default? [Yes, No, Partial]	YES
Do you provide your users with a password manager software?	NO
Do you manage privileged accounts using tooling? [Yes, No, Partial]	NO / Optional
Do you have a security operations center established, either in-house or outsourced? [Yes-24x7, Yes-working hours, No]	YES 24x7

RANSOMWARE CONTROLS	
Pre-screen e-mails for potentially malicious attachments and links?	YES
Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if they are malicious prior to delivery to the end-user?	YES
Can your users access email through a web application or a non-corporate device?	YES
Do you enforce MFA for users accessing email through a web application or a non-corporate device?	YES
Do you allow remote access to your network?	YES
Do you use MFA to secure all remote access to your network, including any remote desktop protocol (RDP) connections?	YES
Do you use a next-generation anti-virus (NGAV) product to protect all endpoints across your enterprise?	In Process
Do you use MFA to protect access to privileged user accounts?	NO
Do you use a data backup solution [Daily, Weekly, Monthly]?	YES Daily
Do you use a Cloud syncing service for backups? (E.g. Dropbox, OneDrive, SharePoint, Google Drive)	NO
Estimated amount of time it will take to restore essential functions in the event of a widespread malware or ransomware attack within your network?	1-3 Days
Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months? [Yes, No, Partial]	YES
Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware? [Yes, No, Partial]	YES
Backups are secured with different access credentials from other administrator credentials?	YES
Are your backups encrypted?	YES
Backups are kept separate from your network (offline/air-gapped), or in a cloud service designed for this purpose. [Yes-fully offline, Yes-cloud service, Yes-partially offline, No]	YES Fully Online

CYBER LIABILITY cont.

PHISHING CONTROLS

Do any of the following employees at your company complete social engineering training? (No, Yes: All, C-Suite, Financial Responsibility, Other select)	YES
If "Yes" to question A. or B. above, does your social engineering training include phishing simulation?	NO

EMAIL SECURITY

Provide a quarantine service to your users?	YES
Strictly enforce Sender Policy Framework (SPF) on incoming e-mails?	YES
How often is phishing training conducted to all staff (Monthly, Quarterly, Annually)?	N/A
If Yes: Do you use the o365 Advanced Threat Protection add-on?	YES

OTHER SECURITY PREVENTATIVE MEASURES

Note any additional steps your organization takes to detect and prevent ransomware attacks (e.g. segmentation of your network, additional software tools, external security services, etc.).

A FEW TYPICAL NON IT QUESTIONS

Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form?	
Does your organization send and/or receive wire transfers?	
If "Yes", does your wire transfer authorization process include the following:	
A wire request documentation form?	
A protocol for obtaining proper written authorization for wire transfers?	
A separation of authority protocol?	
A protocol for confirming all payment or funds transfer instructions/requests from a new vendor, client or customer via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the payment or funds transfer instruction/request was received?	
A protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information or mailing addresses) via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the change request was received?