IS YOUR BUSINESS OR ORGANIZATION PREPARED TO RESPOND TO A CYBER ATTACK?

An Incident Response Handbook for Executives and Business Leaders

By Michael Moran, Affiliated
www.aresgrp.com

AFFILIATED
Cybersecurity, Compliance, & Managed IT Support

TABLE OF CONTENTS

A QUICK OVERVIEW

Let’s get right to the point: A cyberattack, or a breach of your data and IT systems, is expensive: lost revenue, unforeseen expenses, and damage to your reputation.

Our e-book summarizes the knowledge we’ve gained assisting organizations to prepare against, and respond to, these types of events. It is written with business and organization leaders in mind, and is designed to provide guidance as you contemplate your organization’s needs, and your response readiness in the event of a cyberattack or breach.

Let’s start with a few definitions:

Incident vs. Breaches

Incident:
A security event that compromises the integrity, confidentiality or availability of an information asset.

Breach:
An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

An organization can have both; all breaches are incidents, but not all incidents become breaches.

States have data protection laws specifying that certain types of personal data must be protected. In the event of a breach, there are mandatory rules regarding notifications, and increasingly, remedies for those affected. These laws are in addition to those regulatory requirements for data protection and security (HIPAA, NIST, PCI, etc.). We will use incident as the base term in this document.

KEY TAKEAWAYS FOR LEADERSHIP

Overview

Effective incident response is a complex undertaking, requiring substantial planning and resources. Its steps parallel the more traditional Disaster Recovery Plan, but is focused on issues resulting from an increased cyber threat landscape. An Incident Response Plan is a part of your overall Cybersecurity Plan.

The recommendations in this guide are intended to educate, and assist, organizations in establishing computer security incident response plans that will enable you to manage incidents efficiently and effectively.

Be Prepared

Being prepared is key — knowing what to do (and what not to do) is critical information to have before a cyber event occurs. The cost of trying to fix an incident, without being prepared, is significantly higher than just the cost to get your systems back up and running. By having an effective plan in place, the disruption and productivity loss can be limited. Regulatory and data protection violations, civil litigation, and reestablishing your reputation adds significant cost to the incident remediation.

Checklists & Processes

Having standardized, validated organizational processes prevents issues, reduces damage to the organization, and limits incident cost.

Effective Communication is Vital

Collaborative discussions with your team regarding how to handle communications surrounding the incident are critical. This includes internal communications among leadership and with the remediation team, interactions with customers and vendors, communications with key partners (legal, insurance, IT partners, etc.), and addressing the media (when required). These are vital when managing the issue and recovering effectively.

Training

Everyone in the organization needs to be trained. Incident roles and actions must be practiced so that responses are not foreign when an attack happens.

WHAT IS AN INCIDENT RESPONSE?

Key Terms

Event: Any observable occurrence in a system or network

Adverse Incident: Any event with negative consequences or impacts

Security Incident: A violation, or imminent threat of violation, of computer security policies, acceptable use policies, or standard security practices

Examples of a Security Incident

- Users are tricked into opening a “UPS Notice” sent via email that is actually malware; once opened, this malware has infected their computers and established connections to an external host
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a ransom
- A user exposes sensitive information on social media or other sharing sites
An attacker uses a botnet to send high volumes of connections to a web server, causing it to crash (Denial of Service)

WHY ORGANIZATIONS ARE UNPREPARED

The goal of incident response planning is to enable IT departments, and organizations, to respond effectively as they manage the events that occur during, and after, a cyberattack or security incident.

Many internal IT teams don't have a formal IT incident response plan in place to cope with any disruption to the business. Incidentally, a majority of IT consulting firms (Managed Services Providers, small hosting facilities, etc.) don't have one either. If you are working with a provider (whether they cover all, or even part of your IT functions), you need to ask "Show me your Incident Response Plan" to know that they are positioned to help you.

By and large, internal IT teams for small and mid-market organizations are ill-equipped to craft, and implement an incident response plan. They are usually qualified professionals that are operating at capacity to meet demands (user support, application support, hardware and software installations, IT operations activities, security operations, etc.). Having limited time and resources at their disposal, they haven't the bandwidth to invest in learning how to prepare a plan, develop and compile the documentation, and train to respond effectively to an actual incident.

All too often, managed IT services are delivered with thin profit margins, and providers are focused on the day to day support issues from their customer's users – not on fully managing back end operations and planning programs. Asking to review the Incident Response Plan from your current provider, or team, is a reasonable expectation considering you have trusted them to provide your IT services.

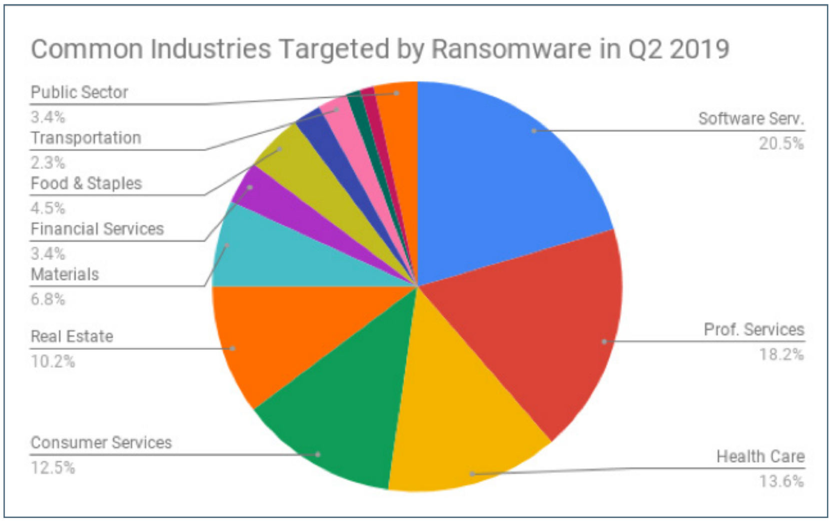
THE MODERN THREAT LANDSCAPE

The #1 cyber security threat for businesses today continues to be ransomware. A recent U.S. Government Interagency Report claimed that 4,000 ransomware attacks take place every day — and that number is likely to continue increasing.

As an example, in Q2 of 2019, the average ransom payment increased by 184% to $36,295, as compared to $12,762 in Q1 of 2019. This escalation reflects the growing prevalence of more diverse variants of ransomware which allow attackers to rapidly inflate their demands.

Cyber Security Statistics & Data Points:

- 60% of attacks target small/mid-size organizations
- 27% of breaches are caused by inadvertent misuse of data by employee's vulnerabilities (e.g. phishing e-mails)
- 55% of businesses report 1 or more breaches
- Research points to users being significantly more susceptible to social attacks they receive on mobile devices
- Lack of cyber security training fuels the success of ransomware
- 33% of the businesses surveyed admitted they do not back up their systems effectively (which could minimize downtime)
- Less than 1 in 3 attacks are reported to the authorities
- 33% of firms required 3+ days to recover from an attack



COVEWARE

It's not a question of if, it's a question when your organization will have an incident.

WHAT IS THE REAL COST OF A CYBER INCIDENT?

Consider this example from an actual customer:

Commodity business with an annual revenue of $25,000,000.
(Sales come through an order desk call center, and a website)

- 100 employees with average cost of $150/day
- Hard downtime cost = $15,000 in staff cost per day

$100,000/day revenue cost ($25mm/250 workdays per year) and assuming 20% lost

- Average customer order: $1,000
- Average annual spend: $20,000
- Expected customer life: 3 years

Potential lifetime LOST customer value???

$1,200,000 (or more, per day down)

For other industries:

- What does it cost to miss filing a motion for an important client?
- What happens if you can't deliver a $350,000 RFP on time?
- What does it cost to have to re-schedule patients for 1, 2, or more days?

Planning begets awareness; preparation begets readiness.

STEPS IN AN INCIDENT RESPONSE PLAN

Proper planning and preparation are essential to a successful incident response. When you prepare well, you have a better understanding of what's needed for a particular course of action.

Being prepared for a cyber security attack, or a data breach, not only reduces the business risk, but also the potential damage associated with the attack, including the difficulty of managing the response and recovery times.

Planning begets awareness; preparation begets readiness.

1. Preparation

Understanding what you have, and what needs to be protected. Establishing your processes for the protection detection and recovery stages – how executed, verified daily IT operation processes can both prevent and prepare you for a faster response and recovery.

2. Communication Plan

What should be shared, with whom, and how it is communicated is very important during an incident. Being prepared beforehand improves your efficiency, and how you are perceived both internally and externally.

3. Remediation Plan

How your team will identify the issue, analyze it, isolate it, fix it, recover from it, and capture the information for appropriate post-incident review.

PREPARATION PLAN

Environment, processes, IT operations planning

Central in the prevention of many incidents are having defined expectations from leadership, well documented and validated processes, in addition to the appropriate tools to protect your organization.

At a high level, these items need to be addressed:

- Defined Leadership expectations for IT performance, readiness, threat tolerance, compliance, outage time, and investment
- Current documentation of the IT environment and assets
- Multi-location, regularly tested backup systems
- Periodic Risk Assessments ensuring new exposures are identified
- Security Program for protection from, and detection of, issues/threats
- Verified Malware Prevention at all levels (devices, hosted systems, servers, networks, etc.)
- Validated Operating Systems patching process to current levels
- Intelligent Firewall device with appropriate configuration and security subscriptions
- Continuous User Security Awareness Training Program
- Appropriate policies and procedures to address permitted use, passwords, operational access, IT operations management, etc.

As a leader you don’t need to know all the details. You just need to verify that your IT team has you covered.

COMMUNICATION PLAN

Developing a communication plan

This communication plan is covers both internal team members, and any relevant outside parties. **Depending on the scope of the incident, the response team may need to communicate with outside parties such as:**

- Law Enforcement
- ISPs/Cloud Application Providers
- Software / Hardware Vendors
- Media Representatives
- Other Incident Response Teams (IT Providers, etc.)
- Customers
- Legal and Insurance

The key here is to develop your plan, and execution strategy before it is needed.

COMMUNICATION PLAN (CONTINUED)

A Communication Plan should document:

- Who is authorized to communicate with each type of party (inside/outside) and what can and cannot be shared
- If/When you should hire an outside communication
- Management firm, as well as guidelines to engage (or hire) your legal team
- Required staff training and processes for handling the media, your customers, and any 3rd party entities
- The importance of not revealing sensitive information
- How to handle contact, communication, and interactions with authorized team members
- A statement of the current status of the incident, so all interactions are up to date and consistent
- Internal communication status plans to address the status between the remediators, leadership, and staff to keep your teams abreast of the situation

REMEDIATION PLAN

Develop a list of items or issues to fix in an environment

It is paramount to remediate the problem that the ransomware or breach exploited in the first place – and ensure the issue is fully contained and fixed.

Ensuring it does not happen again is commonly a user behavior or training issue. In cases such as these, additional awareness training, coaching or simulations can be implemented. In other cases, new technology needs to be put in place. For instance, if backups were found to be inadequate, the company would back up more data, or back up more often.

The incident, though unfortunate, should result in some improvement that the organization can make to be better prepared for subsequent incidents.

At a high level, these steps need to be addressed:

- Analyze the reported incident to determine if something occurred, and then determine what was actually affected.
- Rebuild any system that was infected, and that could not be cleaned
- Any system with activity that looks like a threat, and could not be identified, should also be wiped and rebuilt
- Maintain forensic data that may be requested by insurance and investigators
- Tighten network security to restrict the same attack from happening again (once a network is attacked, it is often attacked a second time)
- Restart scheduled backup routine ASAP
- Use a phased approach so that remediation steps are adequately prioritized
- For larger organizations this takes time – Do not rush the process

POST-INCIDENT ACTIVITY

- Lessons learned
- Debrief and document learnings
- Adjust operations based on findings
- Use data collected to improve response and prevention
- Determine evidence retention for the incident
- Prosecution
- Data retention
- Cost Analysis

Addressing a Data Breach From a Cyber Attack

Now that you have recovered from the incident, you need to evaluate the quality or level, and quantity of the data that could be, or has been, compromised.

Understanding the quantity of records affected will need to be assessed by evaluating each impacted device (workstations, servers, printers, copiers, fax machines, medical devices, etc.). Once you have this information, you can begin to determine the quality of the compromised records.

For example, a 250-employee manufacturing firm that only sells to other companies is attacked by ransomware that affects all workstations and the company's servers. Payroll records for all 250 current, as well as 300 previous, employees are located on 2 workstations in multiple files, and stored on server drives. The company has had a 550-record data breach, and needs to act according to the appropriate data protection laws in their state to notify the affected people, and as required provide remedies.

Each state (and many industries) have data protection laws that affect personally identifiable data. To act accordingly, you must understand the reporting requirements, timelines, and remedy information required by your state (or the state in which the affected people reside) in addition to any regulated industry requirements.

Failure to do so will result in fines and penalties to your organization.

Managing the data in the manner that does not provide reasonable care will expose your organization to potential civil liability judgements.

You also risk non-reimbursement of claims from your cybersecurity insurance provider.

Create a Plan, Execute the Plan, Exercise Due Care, Be Prepared.

What To Do Immediately Following a Cyberattack

Call your organization's insurance company. They will explain their requirements, and outline any steps that may need to be taken to protect forensic data or evidence. You want to support, not hinder, your ability to collect an insurance claim.

- Review your organization's business continuity or disaster recovery plan (if you have one). There may be specific requirements and action items mandated by certain policies, leadership, or industry regulations(s).
- Begin the Communication Plan – Communicate, or reiterate, the company's rules of disclosure to its employees, including what should or should not be communicated via public channels like social media, to the press, or with clients. A standard recommendation is that nothing is permitted to be disclosed until the company releases a formal statement (generally after the facts of the event have been gathered and properly analyzed).
- Back up everything—even encrypted or infected computers—to create a recovery path in case the containment or remediation steps destroy data (or in the event that decryption fails and a recovery key is discovered after the event has occurred). There have been cases where the threat actor releases the decryption key months after an attack has stopped paying dividends.

1. Containment (actions for the IT Remediation Team)

- Run a scan from the internet to look for anything unusual (e.g. ports) that shouldn't be open in the firewall.
- Deny all international traffic in the firewall.
- Deny all inbound traffic across RDP or other remote access tools to the client site. If necessary, enable VPN access first, then RDP across the VPN-protected connection. If possible, unplug your internet connection at the router until you have regained control of the network. You can also unplug all switches on the network to help avoid lateral movement of the threat and to isolate segments of the network as you work on containment.
- Check all security and system logs for any unusual activity.
- Test your backups, and if possible, create a manual set and store them off the network.
- Check for stolen credentials on the Dark Web.
    - Check local and domain accounts for any changes, or new accounts you weren't expecting to see. Remove or disable any old accounts, and verify ones created recently as being expected.
    - Use your detect & respond tools (if implemented) to help hunt for, and isolate, the threat, provide additional visibility, and aid in preventing further spread of the attack.
    - Analyze and provide additional visibility into the activity going through the firewall, in Active Directory, and on endpoints.
    - Receive authorization (in writing, email or text from the client or insurance provider), before moving to the Remediation Steps.

2. Remediation

Before beginning these steps, unplug the internet connection and either unplug the switches on the network or disconnect all machines (including servers). Consider also removing the gateway IP address from DNS temporarily.

- Clean a domain controller (possibly in safe mode) of the infection.
- Disable Autorun on all systems on the network using a Group Policy Object (GPO) in Windows. For GPO visit goo.gl/yBCNeg to read: How to Disable the Autorun Functionality in Windows Note: It is strongly recommended to disable the Autorun feature using Group Policy from the Domain Controller.
- Disable Windows Task Scheduler on all systems on the network. For more information visit goo.gl/dZGEPK to read: How to Prevent a User From Running Task Scheduler in Windows Note: It is strongly recommended to disable the Windows Task Scheduler using Group Policy from the Domain Controller.
- Reset all user passwords to a default password, then share that new password verbally around the office so users can reset their passwords. Do not email it out and be sure to force users to create a new password from the temporary password you set. If you only force password changes, then there is a chance the threat actor will reset their compromised account and still have access to the network.
- Reset all device passwords, including switches, routers, firewalls, VPNs, IDS devices, etc.
- Bring up one server at a time, clean it, and if it's not a required server, shut it down until you have completed cleanup of the entire network.
- Bring up one workstation at a time (of the network) and clean as needed. Reboot several times looking for a return of the infection.
- Check your backups again. You can never have enough good backups.

3. Recovery

- Restore from clean backups
- If clean backups do not exist, consider the ransom demand. That decision is entirely up to you, your legal team, your insurance company, and the data owners.
- Scan the network one more time using relevant tools with an updated security scanning engine.
- Once the network is back online, run a new backup job and backup all critical data before allowing users on the network. In certain cases, this may be a time-consuming effort. It is well worth the exertion versus running the risk of a second, or repeat, infection.

4. Debrief

- Review and document the entire incident
- Debrief with the team fully, and work to design and implement an updated security plan configured to help defend against this type of attack in the future.

MEDIA & PUBLIC RELATIONS RESPONSE

In addition to the obvious, major costs and risks associated with managing a security incident, the potential damage to brand and reputation (and loss of customer trust) can be equally, if not more, damaging.

Beyond the impact on your reputation, a poorly managed security incident can affect employee morale, as well as lead to regulatory scrutiny, or even litigation.

Expectations are changing as the frequency and severity of cyberattacks continue to rise. Even organizations with highly sophisticated cyber defense solutions can fall victim to an attack.

Organizations should be judged based on how well they manage, and respond to, an incident, rather than by whether they can prevent one from occurring in the first place. The most well-protected businesses, however, are those that focus on both strategies.

Communicating effectively with all staff, and appropriate outside parties, requires careful planning, as well as an understanding of the unique dynamics of cyber security issues, and what makes them different from crises.

Provided here are several steps you should consider taking now, to be prepared to handle an incident.

What to Say, What Not to Say, and How to Say It.

The reporter’s priorities are the reporter, their editor, rival reporters, their audience, and (lastly) their source: You.

Before speaking with the media, a spokesperson needs to be well prepared:

- Understand the angle so you know why the interview is important to the reporter, and their readers
- Realize how the story will impact your company and stakeholders
- Make sure that your company’s image, and position, in consistently conveyed during every interview

Tips For a Successful Interview

- Prepare by rehearsing with your PR team, or other members of your organization, to become more comfortable with the topic and key messages
- Don’t assume the reporter is an expert on the topic
- Listen carefully before responding
- Remember that quotes, NOT questions, will appear in the article
- Use clear, simple language without jargon
- Stay on topic with the reporter
- Talk slowly
- Assume everything is “on the record” and being recorded
- Never put the reporter’s call on hold
- Vary the inflection and tone of your voice to add variety
- Never say “no comment”
- It’s okay to take pauses before you answer; don’t be pressured by silence
- Communicate your company’s key messages
- Be straightforward; and if you don’t know something, be honest and offer to follow up at a later time
- When a reporter presents several questions at once, focus on the question that you want to answer
- Don’t speak negatively of any other organization
- Stick to the facts rather than opinions, and never speculate
- Use anecdotes or real examples when possible
- Summarize at the end
- Be available for fact-checking or to provide more information after the interview
- Don’t assume you’ll have a chance to review before publication

Handling Questions - Be Prepared for Standard Questions

- How did this happen?
- What precautions did you have in place to protect the organization?
- What data did they get?
- Who was affected and how will you be assisting them?
- How will you keep this from happening again?

Final Thoughts on Handling a Media Interview

- Remember, no reporter writes a story that includes a list of questions they asked the interviewee. It’s your answers that matter, because that’s what makes the story.
- One of your key goals is to appear fresh and spontaneous during the interview, not rehearsed or scripted.
- Everything you say to a reporter — whether before, during or after the interview — can affect the story.
- Even if you disagree with a reporter’s story about your company, it doesn’t mean the reporter hasn’t done his/her job.

Why Affiliated For Your IT Security Solutions?

At Affiliated, we help our customers align their technology assets and resources with their business plans to achieve their goals… faster… giving them the tools and information they need to make progress every day. We can do that for you, too.

Our security and compliance services are designed around your needs; we provide our services in layers, wrapping your assets in multiple forms of protection and oversight.

We start with a discussion about your priorities and your risk tolerance and then provide the appropriate assessment to determine your position; develop a management plan, then offer remediation services and ongoing service and compliance program offerings to help your team add security and compliance awareness, protection, detection, and response to your DNA.

Mike

Mike Moran
President, Affiliated

Affiliated provides:

- A proven set of processes with tailorable solutions from risk assessment through remediation and on-going Security Programs.
- Security Assessments and processes for addressing the four main components of a focused IT security program—Identify, Protect, Prevent and Detect
- Monitoring and reporting tools plus services. Our tailorable solutions can include base or advanced intrusion detection and log management solutions; issue tracking and management options to ensure timely response and follow through.
- On-going Security Programs to review progress, re-assess risks, make adjustments to your environment, and demonstrate a continued path of action to keep you secure.
- User Awareness Training Programs for your staff.
- Policy and Procedures frameworks and assistance reviews and actual documents to help you implement the appropriate level of process to protect you, your organization and your data.
- A team approach to addressing your IT needs – Microsoft, Virtualization, Storage, Network, Security, and Cloud specialists engaged to help you accomplish your goals.
- Leadership insight to help you make better informed decisions.
- On-site and Off-site backups of your systems and data on a scheduled basis to minimize data loss, as well as daily verifications, weekly verifications and test restores.

START A DISCUSSION TODAY…..

Contact us at 614.495.9658 to start a conversation about your priorities and how we might help you ensure you cybersecurity and compliance activities are aligned with your business goals.