TECHNICAL • COMMUNICATIONS • OPERATIONS • LEGAL

# INCIDENT RESPONSE REFERENCE GUIDE

First aid tips and preparation guidance to limit damage and protect your mission

Microsoft



Building a better working world

Edelman

# First, Do No Harm

A critical principle of medicine applies equally well to cybersecurity incident responses – Do No Harm.

Organizations face many pitfalls that can dramatically increase the negative impact of an incident.

This guide is designed to help you manage a cybersecurity incident while avoiding common errors, increasing both the effectiveness and efficiency of your incident response efforts.

# Incident Response Reference Guide
## First Aid for Major Cybersecurity Incidents

### CONTENTS

Introduction

Preparation
- o Technology
- o Operations
- o Legal
- o Communications

During an Incident
- o Operations
- o Technology
- o Legal
- o Communications

### KEY TAKEAWAYS

**Preparation pays off** – Preparing for a major incident can reduce damage to the organization, as well as reduce incident cost and management difficulty.

**Operationalize your incident management processes** – Managing major cybersecurity incidents must be part of standard business risk management processes.

**Coordination is critical** – Effective cybersecurity incident management requires collaboration and coordination of technical, operations, communications, legal, and governance functions.

**Stay calm and do no harm in an incident** – Overreacting can be as damaging as underreacting.

# Overview

Unfortunately, most organizations are likely to experience one or more major incidents in which an attacker has administrative control over the IT systems that enable your business processes and store your critical business data.

This is a "first aid" style of guidance for cybersecurity to help you:

**1. Prepare for a Crisis** – Reduce risk to your organization with key preparations.

**2. In a Crisis** – Immediately limit potential damage to your organization.

This includes tips and guidance for technical, operational, legal, and communications aspects of a major cybersecurity incident.
While these top-level tips and practices may be valuable in managing a crisis, each incident is unique and complex. This first aid kit is not designed to provide complete and response and recovery guidance. There are no guarantees, expressed or implied, in this document. For comprehensive guidance and specialized advice, we recommend the following:

- You should consider engaging professional assistance for an active major incident.
- You should review NIST Special Publication 800-184 "Guide for Cybersecurity Event Recovery" for additional preparation guidance http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

## TARGET AUDIENCE

This guidance is primarily targeted at individuals in the roles of Chief Information Security Officer (CISO), General Counsel, Communications/PR Lead, and Chief Information Officer (CIO) and immediate colleagues, though many other roles and stakeholders will also find this information valuable.

# Introduction

Many organizations will experience a major incident or must respond to difficult questions about preventing, detecting, and successfully managing a cybersecurity attack from customers, partners, and the board of directors.

57%

of responders have had a recent significant cybersecurity accident.

87%

of board members and C-level executives hve said they lack confidence in their organization's levels of cybersecurity.

A 2016-2017 EY survey showed that 87% of board members and C-suite members lack confidence in their organization's level of cybersecurity.

This document is designed to help you better manage these challenges, improve your program with the benefit of our experience, and instill confidence in your ability to manage a major incident. This is based on our collective experiences across a wide range of Fortune 1000® companies and government agencies.

Given the recent spike in cybersecurity threats and the difficulty of defending against them, organizations must focus on how to get the most return on their security investments. The greatest security return on investment will come from prioritizing your security efforts and budget to increase an attacker's cost, as this will deter opportunistic threats and slow (or ideally stop) determined adversaries.


Preparing for and executing a well-planned response can increase an attackers operational cost and dramatically reduce the business impact of a major cybersecurity incident to your organization.

# About Us


Microsoft has been helping enterprise customers discretely investigate and recover from major incidents for over a decade. Additionally, Microsoft provides secure products and platforms, security products and features, guidance like this documentation, and cybersecurity consulting solutions to help our customers. Primary contributors are Mark Simos, Lesley Kipling, and Matt Kemelhar.


Edelman's Data Security & Privacy helps companies navigate the increasingly complex environment surrounding the collection, use, and protection of corporate and personal data. The group assists companies by enhancing trust and advancing brand, reputation, and competitiveness through communications and stakeholder engagement. We work with companies across a variety of sectors to prepare for data incidents, manage security and privacy issues, influence the policy agenda, and define leadership positioning. Primary contributor is Leigh Nakanishi.


EY Cyber Threat Management services, delivered through the Advanced Security Centers help clients complicate (increase effort necessary for threat objectives to be completed), detect, and respond to real-world attacks in the context of their own business and improve their overall cybersecurity posture. These services can be delivered through a traditional advisory approach or a managed service offering through Cyber as a Service. Primary contributors are Chris White and Bryan York.

# Major Cybersecurity Incidents

A security incident is an event that affects the confidentiality, integrity, or availability of information resources and assets in the organization. An incident could range from low impact to a major incident where administrative access to enterprise IT systems is compromised (as happens in targeted attacks that are frequently reported in the press).

A security incident frequently results in a breach of sensitive information, but it sometimes results in operational/data destruction instead. A breach of personal information has specific legal requirements in many jurisdictions.

These types of incidents can become very challenging to deal with for organizations that are not equipped or trained to deal with managing a major crisis operation.

Our teams have observed significantly better experiences with managing a major cybersecurity incident for organizations that integrate with existing disaster recovery plans/exercises and use of crisis management mechanisms like the Incident Command System (ICS).

This guidance is focused primarily on the Respond and Recover phases defined in the NIST cybersecurity framework. For guidance on preventing and detecting major incidents, see http://aka.ms/SPAroadmap

# Preparation

*"Fortune favors the prepared mind."*

Louis Pasteur

# Preparation

This section is designed to help you think through and plan key aspects of building or updating your enterprise breach response plan across these key functions:

- Technology
- Operations
- Legal
- Communication

Many organizations are more likely to face disaster related to cyber attacks than to fire, earthquake or flooding.

Good preparation for responding to a cybersecurity attack can significantly reduce the business risk of an attack and the difficulty of managing the response and recovery.

This section provides what preparation elements have the greatest impact on responding to a cybersecurity attack, based on experience.

# Technology

The preparation for response and recovery of a major cybersecurity incident should include steps to protect against, detect, and respond to an incident.


For Protect and Detect preparation, we recommend you follow the Microsoft securing privileged access (SPA) roadmap of technical controls focused on common attack methods used in major incidents at http://aka.ms/sparoadmap

To prepare to respond, we recommend the following:

## GENERAL PREPARATIONS

**Identify High-Value Assets (HVAs)** – You need to identify the critically important business assets and their technical composition (servers, applications, data files, etc.). This inventory of HVA components is critical for recovery plans to rapidly assess, contain/isolate, and recover these critical assets during an incident that spreads through the production environment. This identification will also be useful for prioritizing protective and detective controls for these assets and identifying threats to them.

**Confirm Reliable Software Deployment** – Validate that you can rapidly execute scripts/installers on all endpoints. In our experience, incomplete or unreliable software deployment systems can significantly hamper recovery efforts.

## INVESTIGATION PREPARATIONS

**Threat detection and monitoring capabilities** – Confirm that you have access to tools and skills that allow you to detect advanced attackers in your environment. These capabilities are constantly evolving, but an advanced program currently would include:

- Event correlation and analysis
- Integrated threat intelligence
- User and Entity Behavioral Analytics
- Ability to detect with both Indicators of Compromise for historical patterns and Indicators of Attack for evolving techniques
- Machine learning analytics

The most critical basic detection capabilities are called specifically in the SPA road map (above).

**Investigation and Forensic capabilities** – Confirm that you have access to advanced tools and skills to investigate targeted attacks that include malware analysis and attack activity analysis that can produce a comprehensive attack timeline. You can get access to these capabilities by purchasing tools and hiring analysts or you can retain access via external entities or professional services.

**Track and analyze response costs** – To enable better risk management, you should keep a record of the costs involved in responding to the incident. This should include both direct costs (external services, credit reporting for customers, etc.) and the cost of the time your team spends on investigation and recovery, as well as the negative impact on your organization's business and mission.

## RECOVERY PREPARATIONS

**Validated backup and recovery capability for critical data** – For example, preparing for a destructive attack that deletes or encrypts data (such as ransomware) requires that you have validated your ability to recover critical data using an offline and/or ransomware resistant backup capability (such as Microsoft Azure Backup).

**Create technical documentation/automation** – Write and validate technical documentation (and/or automation) for procedures that are frequently required during a security incident, including:

**Compromised account recovery** procedures that include consideration of

- Levels of confidence on account compromise (active attacker use, account credentials exposed on known compromised host, suspicious account behavior, etc.)
- How to validate whether accounts were tampered with using offline backups, change logs, or other systems of record
- Whether to reset password or rapidly recreate account
- How to handle potential conflicts/integration with the Identity Management system during any account recreation

**Compromised host recovery procedures** for both workstations and servers. This should include:

- Host OS (and Application) rebuild procedures
- Cleaning procedures and criteria for when to clean vs. rebuild (if "cleaning" a host is deemed acceptable at your organization)
- Network segregation and isolation procedures including the ability to
- Search and monitor internet egress point logs for attacker Command and Control (C2) channels
- Block attacker C2 channels at internet egress points
- Isolate high value assets from other endpoints in the production environment (such as compromised workstations and servers) if feasible.

**Network segregation and isolation procedures** including the ability to:

- Search and monitor internet egress point logs for attacker Command and Control (C2) channels
- Block attacker C2 channels at internet egress points
- Isolate HVAs from other end points in the production environment (such as compromised workstations and servers), if feasible.

We have learned that performing password resets and C2 channel blocking alone is ineffective without also detecting and removing attacker malware from hosts

# Operations

Managing a cybersecurity incident is a challenging event full of technical complexities, unknown variables, and elevated emotions. Because of the potentially severe impact on your business operations, a clear business case can be made to divert efforts, resources, and time to conducting the planning and preparation necessary to survive as a business during a cyber incident.

57%

of organizations rated BCM as their joint top priority, alongside data leakage/data loss prevention

In the recent EY GISS survey, 57% of organizations rated business continuity management (BCM) as their joint top priority, alongside data leakage/data loss prevention.

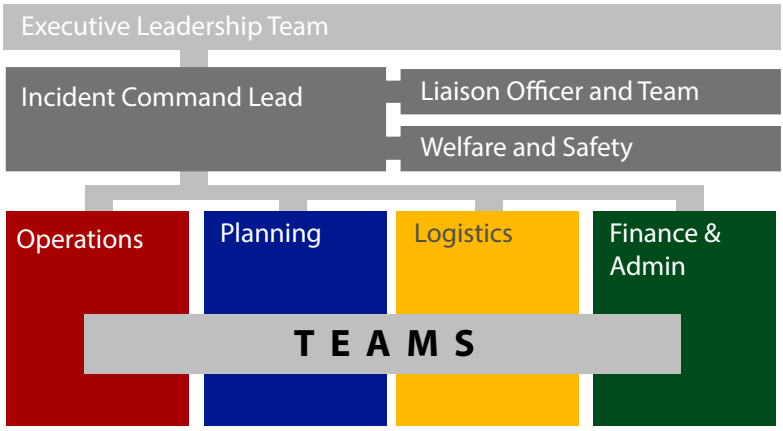
US NIST has published a useful document with many important considerations that highlights the need for preparation:


From http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

This section is designed to help reduce organizational risk by sharing learnings and recommended practices for operations.

## CRITICAL PREPARATIONS

**Adopt Incident Command System (ICS) for Crisis Management** – Major incidents represent an organizational crisis and require a temporary command structure to manage them (if you don't already have a permanent function for this). ICS is used extensively in natural disasters and has proven itself extremely valuable in multiple cybersecurity incidents.
https://en.wikipedia.org/wiki/Incident_Command_System




**Establish a Framework** – Confirm that you have a framework that defines your incident response program.

**Exercise Your Crisis Process** – Establish a recurring schedule to exercising crisis teams and processes on relevant scenarios across all responsibility levels. This schedule should include exercises of individual components as well as tabletop exercises that include all stakeholders (including legal, communications, and organizational leadership). You should also validate non-intrusive technical procedures including backup recovery and threat detection tools during these exercises.

**Emergency Approval Process** – Confirm you have a streamlined emergency approval process for handling rapid changes during an emergency/incident (e.g., authority to judge/approve rapid change proposals and provisions to capture changes and feedback through process afterward).

**Establish Clear Guidelines for Escalation** – Document thresholds for when internal investigations should escalate to specialists and external investigation teams. These can be based on time spent, complexity, unknown malware, specific adversary, etc.

## HALLMARKS OF A STRONG RESPONSE PROGRAM

Because of the complexity of modern organizations, the ideal response program will vary from industry to industry and organization to organization. The general attributes of a strong incident response and recovery program are:

*Strongly integrated with:*

- Business priorities and leadership
- IT Operations
- Business Continuity Management and Disaster Recovery
- Context from internal and external sources

*Continuous learning culture and processes:*

- Postmortems performed and lessons learned integrated
- Regular exercises and red team validation

*Documentation:*

- High level of familiarity with response framework by all stakeholders
- Detailed technical recovery instructions (or automation) for IT and Security Professionals

*Technical Readiness for major incidents:*

- Access to technical proficiency with security systems and business critical systems
- Access to experience on operational, communications, and legal aspects of security incidents (via internal teams and/or partnerships/ retainers with external organizations)

## KEY LESSONS LEARNED

The stronger programs we observe have learned these key lessons:

- Just buying more tools does not equal better security.
- Buying tools without having time and skills to use them is a waste and a distraction.
- Enabling every log source will only drown you in data, increasing the size of the haystack instead of finding more needles.
- Placing your security staff in a dual role with IT operations diminishes their effectiveness.
- You can reduce the cost of an incident by preparing your staff and scheduling availability of required resources.

- Capturing lessons learned is critical to success, as you will see the same attackers and techniques over and over again.

## ORGANIZATIONAL PREPAREDNESS SELF-ASSESSMENT

These questions will help you identify how ready your organization is for a managing a major incident.

## CORE STRATEGY AND ALIGNMENT

- Do you have a good understanding of your HVAs (processes, data, hardware, identities)?
- Do you currently have enhanced controls in place for your HVAs and most likely avenues of attack?
- What are your high-probability attack vectors? What attacker techniques are most likely to be used for agressors to gain initial access and then begin to attempt secondary levels of attack to gain persistence or elevated levels of access?
- Can you measure the impact to your business resources and reputation if you don't invest in preparation?

64%



do not have, or only have an informal, threat intelligence program.

73%



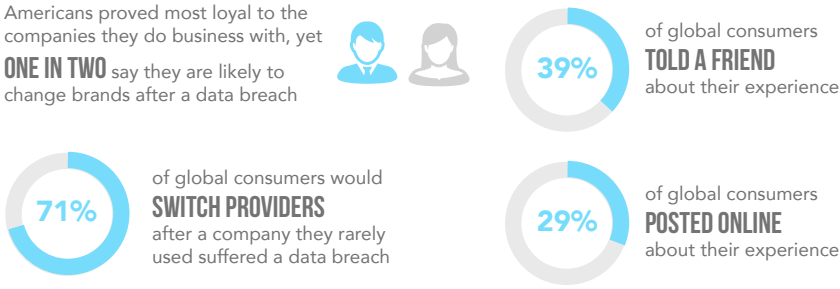
are concerned about poor user awareness and behavior around mobile devices.

## SECURITY OPERATIONS

- Do you have a security operations center focused on detecting and responding to cyber threats?
- Do you have a designated security team and response workflows for handling known threats?
- Do you have a documented, socialized and exercised process in place for incident response?
- Are your people given the proper training and time to investigate cyber threats?
- How effective are your tools at detecting cyber threats?
- For additional context and background, please visit http://www.ey.com/gl/en/services/advisory/ey-cybersecurity

# Communications

Of all the major costs and risks associated with managing a security incident, the potential hit to brand and reputation and loss of customer trust could be the most damaging. According to Edelman's security study, 71% of global consumers said they would switch providers after a company they rarely used suffered a data breach. Beyond reputational impact, poorly managed and communicated security incidents can affect employee morale, as well as lead to regulatory pressure and litigation.




**Expectations are changing** as cyber attacks increase. Organizations are not necessarily expected to prevent security incidents (though this depends on the nature of the risk), but they are expected to effectively manage the fallout of a cyber attack. There is a growing consensus that even organizations with highly sophisticated cyber defense systems can fall victim to an attack, and that companies should be judged by how well they manage an incident rather than if they can prevent one from occurring in the first place.

Effectively communicating around security incidents requires careful planning, as well as an understanding of the unique dynamics inherent in cybersecurity issues that make them different from other types of crises. Unlike traditional crisis issues where transparency and speed are often the right course of action, there is great risk in communicating initial findings and details because the complex nature of forensics investigations make facts fluid. This dynamic leads to an increased potential to disclose information early in the response process that turns out to be incorrect later. This could lead to a loss of credibility, additional news cycles, and increased negative coverage.

Below are several steps organizations should consider taking now to be prepared to handle a potential incident.

## PRIOR TO AN INCIDENT

- **Appoint a communications lead** to be part of the core incident response team and confirm he or she understands the response process and cybersecurity. In the moment of a crisis, precious time and energy is spent identifying who is leading on communications and who will speak on behalf of an organization. There are unique nuances with communicating cybersecurity incidents and investigations that a strong communications lead must understand to be effective. By having him or her as part of the core team, communications and reputation management is more likely to be properly represented during the decision making process.
- **Develop a communications portion of existing incident response** plans, including clear ownership and approval processes. Many companies have technical incident response plans that outline how to investigate and remediate an issue. What's often missing is a communications-centric portion to manage the complex calculus of deciding what to disclose to whom and when.
- **Map the stakeholders** that may need to receive communications regarding an incident including customers, media, partners, regulators, employees and vendors. This includes confirming the company understands its contractual obligations to inform certain partners or customers. Often incidents may not require disclosure to regulators or consumers, but they still need to be shared with enterprise customers in a timely matter. Understanding these obligations ahead of an incident can save valuable time during a live incident.
- **Develop draft media holding statements** and other materials for the major types of incidents that are of most concern to your company. These statements are intended to be used with the press during the early stages of an investigation when many of the details of the issue are still unknown. It's also important to develop key communications considerations for each of the incidents, which can help guide decision-making when an incident occurs. For example, if and under what circumstances the company would pay to remove ransomware and how would they position this decision to key stakeholders.
- **Host a table top exercise** with members from the entire incident response team to test how they would react to the media, customer, and regulator attention due to an incident. These tabletops are often best done in conjunction with outside legal counsel and are intended to focus not on all the non-technical aspects of incident response.

# Legal

Legal counsel increasingly plays a critical role in proactive cybersecurity program development, deployment, and execution. As with any compliance regime, cybersecurity lawyers provide legal advice regarding statutory, contractual, and regulatory duties, as well as recommendations on managing and mitigating legal risk that may result from audits, investigations, or litigation. Experienced regulators now expect that organizations will prepare for an incident and will evaluate their regulatory enforcement decisions through that lens.

The following are some of the key aspects of proactive legal work flows in cybersecurity:

- **Designate a Cyber Lead from Legal.** Much of cybersecurity incident response preparation involves evaluating and managing legal risk. With no overarching cybersecurity law, counsel should draw from a patchwork of statutes (e.g., state notification statues), regulations, government enforcement proceedings, settlements, and guidance, and litigation trends to assess risk. Legal counsel (internal and/or external) should also be positioned to "direct" certain incident response preparation activities and to retain outside forensic and communications experts to maximize the likelihood that their proactive and reactive work is covered by the attorney-client privilege.
- **Review Policies and Public Statements.** If you say you do it, you'd better do it. That goes not only for public representations (e.g., privacy statements, service representations), but also internal security policies. These policies and public disclosures should be regularly reviewed to represent the current state, and avoid unnecessarily grand or definitive statements about a company's cybersecurity program (e.g., "we have bank-level security" or "we have state-of-the-art cybersecurity").
- **Develop an Incident Response Plan.** The Incident Response Plan is the key operational document that pulls together different aspects of a company's response to a security compromise or data breach. Regulators and plaintiffs focus on not only the technical security measures in place, but also the speed, efficiency, and effectiveness of the company's response when facing a cyber attack. Expert cyber counsel craft operationally effective processes that reflect the latest insights from regulators and litigated cases with an eye toward building a narrative of diligence while avoiding inadvertent admissions of liability or creating ad hoc standards that are neither reasonable nor attainable.

- **Conduct Cybersecurity Assessments and Tests at Legal's Direction.** Results from these assessments are among the first requests by regulators and plaintiffs. Because organizations often cannot implement all of the recommendations that arise out these assessments, teams must make risk-based judgments around remediation and mitigation efforts. Legal counsel (inside or outside) should retain cybersecurity consultants to conduct penetration tests, vulnerability assessments, etc., and scope and direct their work in very close collaboration with IT Security, thus protecting related communications, work product, and deliberations under legal privilege. Reports should be prepared sparingly, and only at the direction of counsel to minimize discovery risks.
- **Conduct Regular Board Briefings.** Directors cannot fulfill their fiduciary responsibilities if they are not aware of the risks. Accordingly, boards should be regularly briefed on cybersecurity risks, and provided with sufficient information and expert assistance in understanding and assessing cybersecurity risk, so that they can effectively manage cybersecurity risk.
- **Manage Third Party Vendors.** Third parties with access to the corporate network or personal data about customers/employees expand the attack surface and often represent the "weakest link." During the diligence phase, vendors should be evaluated based on the risks that they present. Agreements should be negotiated to include security standards that vendors must comply with; a clear process on how vendors will investigate, cooperate, and notify affective individuals; and legal protections (indemnification, limitation of liability, insurance, etc.) for when an incident takes place. Finally, organizations should develop an audit, review or certification process to test vendors' compliance with security standards.

# In a crisis

*"There cannot be a crisis next week. My schedule is already full."*

Henry Kissinger

## DURING AN INCIDENT, IT IS CRITICAL TO:

- **Keep calm** – Incidents are extremely disruptive and can become emotionally charged. Stay calm and focus on prioritizing your efforts on the most impactful actions first.
- **Do no harm** – Confirm your response is designed and executed in a way that avoids loss of data, loss of business critical functionality, and loss of evidence. Avoid decisions can damage your ability to create forensic timelines, identify root cause, and learn critical lessons.
- **Be Accurate** – Confirm anything you share to the public and to customers is correct and truthful.
- **Get help when needed** – Investigating and responding to attacks from sophisticated attackers benefits significantly from deep expertise and experience.

Like diagnosing and treating medical disease, cybersecurity investigation and response for a major incident requires defending a system that is both:

- Critically important (can't be shut down to work on it)
- Complex (typically beyond comprehension of any one person)

During an incident, you must strike several critical balances

**Speed:** You must balance the need to act quickly to satisfy stakeholders with the risk of rushed decisions.

**Sharing information:** You must inform investigators, stakeholders, and customers while limiting liability and unrealistic expectations.

This section is designed to lower risk to your business in an incident by identifying common errors to avoid and providing guidance on what actions you can take rapidly that both reduce risk and meet stakeholder needs.

# Technology – Investigation Phase

## CRITICAL SUCCESS FACTORS

- **Must Identify Scope of attack operation** – Most adversaries use multiple persistence mechanisms.
- **Identify Objective of attack, *if possible,*** as persistent attackers will frequently return for their objective (data/systems) in a future attack.

### KEY EXPECTATIONS TO MANAGE

You may never be able to identify "patient zero" as the data required for this may be deleted before the investigation starts (attacker covering tracks, logs rolling, etc.).

## TIPS

- **Don't upload files to online scanners** – Many adversaries monitor instance count on services like VirusTotal for discovery of targeted malware.
- **No modifications** – Unless you face an imminent threat of losing business-critical data (deletion, encryption, exfiltration), do not start recovery operations until the investigation is complete.
- **Don't investigate forever** – You must ruthlessly prioritize your investigation efforts (e.g., only perform forensic analysis on hosts that attackers have actually used or modified). In a major incident where an attacker has administrative privileges, it is impractical impossible to investigate all potentially compromised resources (which may include all corporate resources).
- **Share information** – Confirm that all investigation teams (including all internal teams and external investigators) are fully sharing their data with each other.
- **Access the Right Expertise** – Confirm you integrate people with deep knowledge of the systems into the investigation (internal staff or external entities – like vendors – as needed), not just security generalists.
- **Legal check** – Check with your legal department on whether they plan to involve law enforcement so you can plan investigation and recovery procedures appropriately.
- **Your response capability will be negatively impacted** – Plan for 50% of your staff operating at 50% of normal capacity due to situational stress.

# Technology – Recovery Phase

## CRITICAL SUCCESS FACTORS

- **Don't boil the ocean** – Limit response scope to confirm recovery operation can be executed within 24 hours or less (plan a weekend to account for contingencies and corrective actions).
- **Avoid distractions** – Defer long-term security investments like implementing large/complex new security systems or replacing antimalware solutions until after the recovery operation. Anything that does not have direct and immediate impact on the current recovery operation is a distraction.

### KEY EXPECTATIONS TO MANAGE

The first recovery attempt may not fully succeed, so you may have to try again.

## TIPS

- **Never reset all passwords at once** – Password resets should focus first on known-compromised accounts (from investigation) and potentially administrator/service accounts. If warranted, user passwords should be reset only in a staged/controlled manner.
- **Consolidate execution of recovery tasks** – Unless you face an imminent threat of losing business-critical data, you should plan a consolidated operation to rapidly remediate all compromised resources (hosts, accounts, etc.) vs. remediating compromised resources as you find them. Compressing this time window will make it difficult for attack operators to adapt and maintain persistence.
- **Use Existing Tools** – Research and use the capabilities of tools you have already deployed (software deployment, antimalware, etc.) before trying to deploy and learn a new tool during a recovery.
- **Avoid tipping off adversary** – As practical, you should take steps to limit the information available to adversaries about the recovery operation. Adversaries typically have access to all production data and email in a major cybersecurity incident, but in reality, most attackers don't have time to monitor all your communications. When required, we have successfully used a non-production Office 365 tenant for secure collaboration for members of the incident response team.

# Operations – Investigation Phase

## CRITICAL SUCCESS FACTORS

- **Stay focused** – Confirm you keep the focus on business-critical data, customer impact, and getting ready for remediation.
- **Coordination and role clarity** – Establish distinct roles for operations in support of the crisis team and confirm technical, legal and communications teams are keeping each other informed.

### KEY EXPECTATIONS TO MANAGE

Expectations for the flow of information between stakeholders will vary without clear guidance and input from senior incident response leaders

- **Business perspective** – You should always consider the impact on business operations by both adversary actions and your response actions.

## TIPS

- **Consider ICS for crisis management** – If you don't have a permanent organization that manages security incidents, we recommend using the ICS as a temporary organizational structure to handle the crisis.
- **The show must go on** – Confirm the daily security operations are not completely sidelined to support incident investigations. The normal work still needs to be done.
- **Avoid wasteful spending** – Many major incidents result in organizations purchasing an assortment of expensive security tools in a panic that are never deployed or used. If you can't deploy and use a tool during the investigation, defer acquisition until after the investigation is finished. Also, consider your ability to hire/train/retain people for any rare or specialized skill sets needed to operate or gain value from the tool.
- **Access to deep expertise** – Confirm you have the ability to escalate questions and issues to deep experts on critical platforms. This may require access to the operating system and application vendor for business-critical systems and enterprise-wide components (desktops, servers, etc.).

# Operations– Recovery Phase

## CRITICAL SUCCESS FACTORS

- **Clear Plan and Limited Scope** – Work closely with technical teams to build a clear plan with limited scope. While plans may change based on adversary activity or new information, you should work diligently to limit "scope creep" of additional tasks.
- **Clear Plan and Ownership** – Recovery operations involve many people doing many different tasks at once, so designate a clear project lead for the operation for crisp decision-making and good information to flow among the crisis team.
- **Stakeholder communications** – Work with communication teams to provide timely updates and active expectation management for organizational stakeholders.

### KEY EXPECTATIONS TO MANAGE

Executive and board-level communications for incident response can be challenging if not practiced or anticipated.

## TIPS

- **Know your capabilities and know your limits** – Managing major security incidents is very challenging, very complex, and new to many professionals in the industry. You should seriously consider bringing in expertise from external organizations or professional services if your teams are overwhelmed or aren't confident in what to do next.
- **Capture lessons learned** – Build and continually improve role-specific handbooks for security operations, even if it's your first incident without any written procedures.

# Communications

Managing communications during a live incident presents unique challenges when compared to other types of crisis that companies can face. What a company knows about the scope of the information lost, how long attackers have been in the system and confirmation that remediation steps were successful in keeping them out of systems, will drastically change over the several weeks it takes to conduct a forensics investigation. As a result, there is a real risk of communicating inaccurate information regarding an incident that can ultimately lead to greater reputational damage for the organization.

## CRITICAL SUCCESS FACTORS

While the fact pattern of each incident will require its own strategy, there are several key principles to keep in mind when making these decisions.

- **Focus on actions not outcomes.** Early in an incident, focus communications on the actions your company is taking to investigate and remediate the security incident. This often includes steps like notifying law enforcement, hiring forensics experts to help in the investigation and any general steps being taken to remediate the issue. Avoid disclosing numbers or otherwise scoping the incident until there is forensic certainty around these facts.
- **Keep customers as your north star.** In all messages, focus on how you are helping to protect customers versus going into detail about how the incident happened or who was behind it. Often the media will want to know more details about the attack itself or other facts that would help produce a more interesting or sensational story. However, these details often do little to help address customers' concerns or needs. Focusing on providing actionable guidance is likely to be more helpful to your customers, as well as regulators who are often most interested in how the company is protecting its constituents.
- **Keep media interactions transactional.** The goal during a security incident is to contain news coverage of the event and confirm that the key messages of the company appear in stories. The most effective way to achieve these goals is to provide the media with written statements and only grant media interviews with a spokesperson if necessary.

- **Leverage your owned properties.** Creating a single online destination where those interested in an incident can get accurate and updated information can help streamline communications. The information posted on this site can include a customer message from company leadership, Q&A we expect customers to ask, as well as links to other resources that may be helpful to customers.

## OTHER COMMUNICATIONS ACTIONS

Effectively managing communications goes well beyond just sharing the right external messages. Several other actions must also be considered as part of an effective response process.

- **Brief internal audiences.** Confirm that any customer-facing employees are briefed about the incident and provided with the appropriate talking points or escalation processes, should they get questions.
- **Monitor the conversation.** Develop crisis-specific traditional and social media monitoring to detect media leaks early in an investigation and then to understand the sentiment once an issue is disclosed. Without a good accounting of the conversation, it's difficult to make decisions as an incident unfolds.
- **Consider steps to regain or earn trust.** While not always required, it's important that your company consider if there are steps it should take to regain customer trust after an incident is concluded.

For more information regarding communicating about security incidents, please visit http://www.edelman.com/expertise/data-security-privacy/.

# Legal

A cybersecurity incident presents a variety of challenges in terms regulatory compliance, statutory and contractual notification obligations, and managing risk of ensuing litigation and regulatory enforcement proceedings and investigations. As a result, legal counsel increasingly plays a critical role in incident response, as well as proactive cybersecurity program development, deployment, and execution.

Early engagement of legal counsel to direct an investigation can substantially assist in identifying these obligations and managing legal risk from regulators, plaintiffs, shareholders, and industry groups.

There are several key principles to keep in mind for compliance with legal obligations, while managing legal risk:

- **Maintain Confidentiality and Protect Privilege.** Legal counsel (internal and/or external) should be positioned to direct the investigation and response efforts, generally in close partnership with the IT security lead, to identify legal obligations and manage risk. With counsel leading the investigation, communications and work product are covered by legal privilege, which adds a significant level of confidentiality protection to the investigation and response efforts. Legal should further retain cybersecurity and communications experts necessary for response, thus covering their work product and communications under the privilege. The privilege creates a "safe place" for responders to facilitate the fact-finding mission and thoughtful discussion regarding risk, without fear that these deliberations will be second-guessed by regulators and plaintiff's counsel.
- **Identify Legal Statutory, Contractual, and Other Obligations.** Statutory legal obligations are constantly shifting as statutory notification obligations are amended and (re)interpreted, changing the data elements and events that trigger notification obligations, and creating so-called notification safe harbors. Moreover, contractual and industry rules often are broader than statutory obligations and not subject to safe harbors. The decision to notify – as well as what to communicate – is made even more challenging by the reality that forensic investigations are often inconclusive and the evidentiary record imperfect. Consider these judgments carefully in light of changing legal interpretations, as well as accepted and expected practices.

- **Take Care Regarding Post-Breach Actions/Statements.** Understanding what to say – and what not to say – is critical to managing legal risk. Plaintiffs regularly use post-incident actions and communications to make arguments about the nature of the incident, the scope of affected individuals, and harm that have keep their suits alive in court. In addition to communications and messaging requiring significant and substantive input from the communications team, all communications and post-breach accommodations to affected individuals should be carefully vetted by legal.
- **Engage Law Enforcement.** Engaging law enforcement is now a key consideration in incident response. Not only is it often an important piece in the communication narrative, but it is often required depending on industry (for example, certain government contractors) and type of data affected (for example, by major card brands in the case of a credit card breach). Properly facilitated law enforcement engagement can also sometimes be leveraged to delay statutory notifications, gain additional information regarding the incident, and help determine root causes and/or data compromised. Legal should coordinate such outreach, at a minimum, to negotiate and manage legal process law enforcement uses to gain information for its investigation.
- **Keep Executives/Board Members Adequately Informed.** Increasingly, shareholders and regulators are scrutinizing C-suite and board members involvement in and oversight of cybersecurity incidents. Updates to executives and board members must balance the quality and quantity of information to enable them to carry out their fiduciary responsibilities and exercise business judgment, while avoiding overloading them with technical details.

# Notes

# List of References


1. National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 January, 2017 https://www.nist.gov/cyberframework
2. National Institute of Standards and Technology, https://www.nist.gov
3. National Institute of Standards and Technology Guide for Cybersecurity Event Recovery https://doi.org/10.6028/NIST.SP.800-184
4. Microsoft Securing Privileged Access Roadmap, http://aka.ms/sparoadmap
5. Microsoft Security Intelligence Report, www.microsoft.com/sir
6. EY Global Information Security Survey 2016-2017, http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016
7. Edelman Privacy Risk Index, http://www.edelman.com/insights/intellectual-property/exploring-consumer-attitudes-actions-key-tech-policy-issues-2014/


*"If you protect your **paper clips** and **diamonds** with equal vigor, you will soon have more **paper clips** and fewer **diamonds**."*

–Attributed to Dean Rusk

# Contact Information

Microsoft Enteprise Cybersecurity Group (ECG)
*http://aka.ms/IR*

EY Contact Information/Instructions
*http://www.ey.com/gl/en/services/advisory/ey-cybersecurity*

Edelman Contact Information/Instructions
*http://www.edelman.com/expertise/data-security-privacy/*

For the latest online version of this content, visit
*http://aka.ms/IRRG*