Organization, Documentation, and Coordination: Responding Successfully to a Cyberattack

EXECUTIVE SUMMARY

Recent, high-profile cyberattacks have made it clear that every business and organization must not only protect key systems, platforms, and networks against a potential breach but also be prepared to respond quickly and decisively in the event of such an attack. Responding to a cyberattack effectively requires advance planning as well as a coordinated effort between the internal incident response team, executives, external resources, law enforcement, in-house and outside counsel, forensic firms, and related data-breach resolution vendors. While information security and cyberbreach prevention are key pre-attack priorities, this paper aims to arm companies with practical steps they can take in the aftermath of an attack. These steps include securing existing operations, investigating and resolving vulnerabilities, notifying individuals and government agencies, conducting post-incident analyses, and collaborating and sharing information with key stakeholders. Additionally, although this paper looks primarily at issues facing the oil and gas industry, the information provided and concepts discussed can be applied to a broad range of business sectors.

I. INTRODUCTION

In early December 2020, the U.S. federal government acknowledged that hackers had breached networks and email systems of a number of federal departments and agencies (including the Commerce, Energy, Homeland Security, and Treasury Departments) in a coordinated attack

Please cite as: Heather Hughes, Krystal Pfluger Scott & Ewaen Woghiren, "Organization, Documentation, and Coordination: Responding Successfully to a Cyberattack," *The Legal Framework for Digitization, Technological Innovation, and the Future of Resource and Energy Development"* 7-1 (Rocky Mt. Min. L. Fdn. 2021).

that potentially exposed significant classified material and confidential information.[1] On January 5, 2021, the Federal Bureau of Investigation ("FBI"), the Cybersecurity and Infrastructure Security Agency ("CISA"), the Office of the Director of National Intelligence ("ODNI"), and the National Security Agency ("NSA") issued a joint statement confirming the cyberattack and noting that the Advanced Persistent Threat ("APT") actor was likely Russian in origin.[2]

The hackers appear to have gained access to their targets through software provided by an infrastructure monitoring and management platform called Orion, developed by Austin, Texas-based company SolarWinds. The APT actor utilized a "supply chain attack," a multi-stage strategy that exploits a vulnerability in an entity that lies earlier on the information supply chain as a means of subsequently gaining access to the attacker's higher-value ultimate victim or victims. In this case, when a customer of SolarWinds updated to a compromised version of the company's software, malicious code entered the target's system and enabled the hackers to obtain user rights and move freely within the network.

Although the dust has yet to clear fully, the breach has affected at least 200 organizations around the world[3] — from government agencies and nonprofits to consulting, telecom, technology, natural resources, and even cybersecurity companies. Particularly troubling is that the hackers, according to SolarWinds CEO Sudhakar Ramakrishna, gained access to SolarWinds in early

---

[1] David E. Sanger, *Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect*, N.Y. TIMES (Dec. 13, 2020; updated Feb. 9, 2021), https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html.

[2] *Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Jan. 5, 2021), https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

[3] William Turton, *At Least 200 Victims Identified in Suspected Russian Hacking*, BLOOMBERG (Dec. 20, 2020), https://www.bloombergquint.com/technology/at-least-200-victims-identified-in-suspected-russian-hacking.

September 2019 and may have been able to deliver the malicious code known as SUNBURST hidden within software updates to approximately 18,000 customers beginning in February 2020. Note that the company did not know about the cyberattack until December 1, 2020—over a year after the initial access and ten months after malicious code conduct started.[4]

This incident is the latest in a long series of cyberattacks against organizations and governments worldwide. This is particularly true for the oil and gas industry, which not only relies heavily on third-party providers for a broad range of software and services, but also has seen a number of recent breaches targeted at energy exploration, refining, and distribution companies.

For example, in early 2020, threat actors used a spear phishing link to gain access to information technology ("IT") and operational technology ("OT") systems at a natural gas compression facility of an oil and gas company. While the company did not report any loss of control of systems, it was unable to read and aggregate real-time data during the course of the attack.[5] In late 2019, hackers launched a ransomware attack against supervisory control and data acquisition ("SCADA") systems at five undisclosed U.S. oil and gas facilities. The hackers successfully prevented the systems from viewing industrial equipment remotely.[6]

In its *Global Risk Report 2018*, the World Economic Forum ("the Forum") ranked cyberattacks third on its list of top global risks. In particular, the Forum noted a growing trend in "the use of cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies

---

[4] Sudhakar Ramakrishna, *New Findings From Our Investigation of SUNBURST*, ORANGEMATTER (Jan. 11, 2021), https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/.

[5] *Alert (AA20-049A), Ransomware Impacting Pipeline Operations*, UNITED STATES DEPARTMENT OF HOMELAND SECURITY (Feb. 18, 2020; last revised Oct. 24, 2020), https://us-cert.cisa.gov/ncas/alerts/aa20-049a.

[6] Christian Vasquez, *'Ryuk' malware harmed 5 oil and gas facilities — report*, E&E NEWS (Jan. 27, 2020), https://www.eenews.net/energywire/stories/1062188535.

functioning."[7] The Forum report further noted that the number of reported cyberattacks had nearly doubled over the preceding five years. The actual number of cyberattacks is likely to be much greater, as there is no way of knowing how many attacks go unreported, given many businesses' concerns over retaining investor and customer confidence.

Costs of cyberattacks are also rising. In a 2019 report, Accenture estimated that the average cost of a ransomware attack in 2018 was $645,000.[8] The total expense of such an event can spiral exponentially; for example, while hackers demanded only $50,000 from the city of Atlanta during their March 2020 ransomware attack, the city ultimately paid more than $2.25 million in recovery costs.[9]

Costs for a data breach that does not involve ransomware may be even higher. A 2020 analysis sponsored by IBM and conducted by the Ponemon Institute (the "IBM/Ponemon Institute study"), which surveyed more than 3,200 individuals from 524 organizations that had been affected by a data breach between August 2019 and April 2020, found that the average cost of a data breach in the United States was $8.64 million. Globally, the average cost of a data breach was $3.86 million and the average cost for each exposed record was $146. When personally identifiable information ("PII") was compromised and the cause of the data breach was a malicious attack, the global average cost per record jumped to $175.[10]

---

[7] *Global Risks Report 2018*, WORLD ECONOMIC FORUM (13th ed., 2018), http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.

[8] *Ninth Annual Cost of Cybercrime Study*, ACCENTURE SECURITY (2019), https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf.

[9] Alicia Hope, *Ransomware Costs in 2019*, CPO MAGAZINE (Jan. 15, 2020), https://www.cpomagazine.com/cyber-security/ransomware-costs-in-2019/.

[10] *Cost of a Data Breach Report 2020*, IBM AND PONEMON INSTITUTE LLP (July 2020), https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf.

These costs can grow exponentially. The IBM/Ponemon Institute study found that mega breaches (those with more than 1 million compromised records) cost significantly more, on average, than smaller breaches. For example, the average total cost of a data breach involving 1 million to 10 million records was $50 million; for breaches of more than 50 million records, the average cost was $392 million.

While large, per-breach numbers of exposed records pale in comparison to the total numbers of records breached to date. In a January 2019 study and survey report, Experian reported exposure of 446.5 million records in 2018 alone, and that, cumulatively, at least 4 billion records had been exposed as of June 2019.[11]

Within this context, it is clear that cybersecurity is a top concern for oil and gas companies. Although this paper will briefly discuss information security and cyberbreach prevention as key pre-attack priorities, this paper focuses on workable steps that companies can and should implement following an attempted or successful breach. During this critical, post-event window, companies should undertake key actions that include securing existing operations, investigating and resolving vulnerabilities, notifying individuals and government agencies, conducting post-incident analyses, and collaborating and sharing information with key stakeholders.

It is important to note that, for purposes of presentation, the tactics described below are generally listed chronologically. However, any phase of the data-breach response may, by necessity, overlap with those activities that precede and follow it.

II. SECURE OPERATIONS

[11] *Data Breach Response Guide*, EXPERIAN (2019-2020 ed.), https://www.experian.com/data-breach/.

Immediately upon discovering or being notified of a cyberattack, an organization's board, executives, senior cybersecurity leadership, and other key personnel must take swift action. More than at any other point in the post-breach process, time is of the essence during the initial hours and days following awareness of a breach. Early, decisive action can stop the bleeding, contain potential damage, support evidence gathering, and establish a legal record to help the organization navigate the complex rules regarding notification and disclosures to federal and state authorities, stakeholders, and the public.

Put simply, when it comes to a data-breach response, time equals money. The IBM/Ponemon Institute study found that in the United States, the average amount of time required to detect and contain a data breach was 280 days. When the data breach was caused by a malicious attack, this number grew to 315 days.

However, the same study also found that rapid action can save significant amounts of money. Identifying and containing a breach in less than 200 days offered respondents an average of $1.12 million in savings compared with attacks that took longer to resolve. Securing operations rapidly and thoroughly is the first priority for an organization that has been targeted by hackers.

Before a breach, get the right team on board and in place. Every organization should have an up-to-date incident response plan ("IRP"), a document that establishes roles, responsibilities, and steps to be taken in the face of a cyberattack. An effective plan includes clear, prioritized action items designed to reduce data loss, minimize costs and damages, and set the stage for rapid recovery from the event. The IRP should take into account the operations and needs of different business units within the organization. It should also include specific preparations for a range of scenarios, including external hackers bent on massive ID theft, theft of funds via compromised business emails and spear phishing, malicious code and botnets affecting an entire

system, disgruntled employees who steal key data, lost or stolen unencrypted devices, and cyber-extortion and ransomware. These scenarios and the specific responses to each can be documented in incident response playbooks that should be readily available to the IT and information security teams, preferably in paper form.

The IBM/Ponemon Institute study found that organizations that had created an incident response team and tested their IRPs reduced the average cost of a data breach by $2 million compared with organizations that had not set up such teams or tested IRPs.[12] Though an IRP has multiple components, two elements are vital. First, the IRP should identify personnel responsible for breach forensics. These professionals evaluate how the breach occurred and determine how it can be prevented in the future. Second, the IRP should also identify the response team. In general, the response team should comprise the following:

- Internal leadership, including the chief executive officer, chief information officer, chief operations officer, and chief marketing officer, as well as leaders from all core business units, including human resources, customer support, and public relations.
- Legal counsel, including in-house and outside counsel with experience handling data breaches. Outside counsel can provide an independent, 360-degree perspective on the legal ramifications of the attack and provide guidance on establishing privileged communications and an evidentiary record (the latter is discussed below).

[12] *Cost of a Data Breach Report 2020*, IBM AND PONEMON INSTITUTE LLP (July 2020), https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf.

- Other outside subject-matter experts, including forensic experts, crisis communications firms, breach-notification firms, insurance agents or brokers, and law-enforcement officials.

The IRP should designate a team leader should and assign clear protocols for managing the overall incident response and deploying the IRP. The team leader's tasks include communicating with C-suite executives, coordinating the work of internal and external team members, ensuring that response activities are fully documented, and working with outside officials and law-enforcement agencies to conduct investigations and address required breach notifications. When a breach is suspected, it is the role of the team leader to activate the IRP and begin the response process.

In developing IRPs, incident response teams can take advantage of detailed guidance available on the websites of the National Institute of Standards and Technology ("NIST") and the National Cybersecurity Center of Excellence ("NCCoE").[13]

After a breach, prioritize containment. Within the first 24 hours following a suspected breach or cyberattack, organizations should secure key assets such as physical areas (*e.g.*, offices, laboratories, distribution centers), digital assets (*e.g.*, access codes, passwords, employee credentials), and anything else that has been compromised or may allow the hackers to continue to operate within or control the network.

A primary goal of containment is to stop an incident before it overwhelms resources or exacerbates the damage caused by the initial attack. Depending on the breach's scope, containment may include processes for shutting down entire systems. Such a shutdown should not, however,

[13] Computer Security Resource Center, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY AND NATIONAL CYBERSECURITY CENTER OF EXCELLENCE, https://csrc.nist.gov/publications/sp#800-86.

be decided upon or enacted unilaterally, and never without the clear guidance of experts. For example, with certain strains of ransomware, incident response experts advise that systems should be removed from the networks but not powered off. This course of action can disable certain vulnerable network functions but allow maintenance of other activities.

In some cases, the containment strategy may also include the use of a "sandbox," or an area of the system to which the hackers are diverted without their knowledge, in order to monitor their activity and possibly gather additional evidence.[14] While this may provide additional information, an organization may find itself liable if the attacker uses the compromised system to attack other entities. The organization's system might also be further damaged if the malicious code runs a "ping" process to another host that, should the process fail to complete, automatically overwrites or encrypts all of the data on the original target hard drive. Containment is a complex approach and requires both forensic and legal guidance.

Prioritize the incident. As the company contains the damage, it is important to prioritize the incident.[15] Prioritization allows the organization to allocate and deploy appropriate resources in a timely manner. Further, should multiple incidents occur simultaneously or in close succession, such prioritization will help ensure that the breach with the greatest short- and long-term impacts on the business receives greater attention.

Incidents should be assessed on three axes: functional impacts, information impacts, and recoverability. Functional impacts measure the degree to which the breach will negatively affect business operations and user experience. Information impacts evaluate the degree to which

---

[14] *Computer Security Incident Handling Guide*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Aug. 2012), SP 800-61 Rev. 2, at 35, https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.

[15] *Id.* at 32.

exfiltration of sensitive information may affect the confidentiality, integrity, and availability of the company's information. Recoverability examines the degree to which the company can address and resolve the incident, as well as the time and resources necessary to achieve a partial or complete recovery.

Taken together, these three factors help organizations gain a clearer understanding of the effort necessary to recover from an incident and allow them to weigh response-related costs against the value of recovery. Incidents that have a high functional impact and a high likelihood of full recovery should take top priority. Those that have low-to-moderate functional and information impacts and have a low likelihood of recovery or require significant resources to achieve recovery should receive lower priority, both in terms of resources allocated and the speed of the response.

Gather evidence now (and at every point in the process). The following steps are key to preserving data and information that can be used to help identify the source of the data breach, assess the scope and potential impact of the breach, stop the attack in its tracks, and establish a legal record for law-enforcement investigations, potential litigation, and postmortem reviews:

- Record the date and time of incident or breach.
- Document everything known about the breach.
- Interview all individuals responsible for or involved in activities that were subject to or otherwise potentially compromised by the breach.
- Confirm and execute IRP-established communications protocols for disseminating information to everyone involved in the breach response.
- Assess priorities and risks.

- Work with forensic advisors to initiate the investigation of the breach.

While the primary goal of evidence gathering is to stop the breach, evidence may also be used in legal proceedings, including civil and criminal litigation.[16] For that reason, it is important to document how the response team gathered and preserved this information. Moreover, the response team should ensure that the evidence is preserved in a manner that makes it admissible in court.

The response team can take the following steps to collect and preserve evidence:

- An initial system "snapshot" should be taken to identify the problem and its source before incident handlers, system administrators, and others have inadvertently altered the evidence during the investigation. This snapshot is the optimal way to preserve evidence from an evidentiary standpoint.[17]

- Chain of custody forms, signed by the sending and receiving parties, should detail the transfer of evidence from one person or department to another.

- Detailed logs should include the following:

    - Identifying information, such as location, serial and model numbers, hostnames, media access control (MAC) addresses, and IP addresses.

[16] *Id.* at 36.

[17] *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*, NATIONAL CYBERSECURITY CENTER OF EXCELLENCE (2020), SP 1800-26, https://www.nccoe.nist.gov/library/data-integrity-detecting-and-responding-ransomware-and-other-destructive-events-nist-sp-1800.

- Names, titles, and contact information for all parties that collected, handled, or transferred evidence.
- Time-and-date stamps for each time the evidence was handled.
- Location of the stored evidence.

Develop and implement a communication plan. A general outline of and guidelines for internal and external communications should already be part of the IRP. However, once the company has established the breach's parameters, it can further refine this general guidance. In developing this plan, the company should ask the following questions:

- *Who will be the targets of the communication?* Audiences may include shareholders, law-enforcement officials, customers, vendors, and other stakeholders.
- *Who will speak on behalf of the team?* Depending on the nature of the compromised information, the type and source of the attack or breach, the scope of the attack, and the likely impacts of the breach, the spokesperson may be the incident response team lead, a communications director, an external public relations firm, the chief executive of the organization, or the board of directors.
- *What will the spokesperson say?* Incident response team leaders should consult carefully with their legal advisors and other outside experts prior to issuing any public, formal statements. Pay careful attention to the nature of the information provided as well as the core messaging. Too little information could lead to litigation or loss of public trust; too much information could provide threat actors with information on the status of the response or cause stakeholders to act against their own interests.

To help minimize follow-up and one-off communications, incident response teams can prepare and disseminate frequently asked questions ("FAQ") documents. These can preempt requests for more detailed information and help ensure that the team is providing consistent, approved communications about what has happened, the steps being taken, and the breach's broader impacts.

III. INVESTIGATE AND RESOLVE VULNERABILITIES

Following a data breach or cyberattack, companies often feel pressed to immediately begin the rebuilding process. Although an organization targeted by a breach may be keenly interested in securing vulnerable areas, reestablishing normal operations, and demonstrating trustworthiness, such efforts should not be undertaken prematurely. If systems are rebuilt too quickly and without a full inspection for additional malware, for example, reinfection may occur and the well-intended effort may be for naught. Misguided or hurried repairs might also compromise evidence that is necessary for investigations, litigation, and postmortem reviews.

To avoid premature action, organizations should first consult with forensic experts. These experts can help communicate technical information, guide the breach investigation, help decision makers better understand the enterprise-level risks of any action, and make sure that no further harm occurs.[18]

[18] *Data Breach Response Guide*, EXPERIAN (2019-2020 ed.), https://www.experian.com/data-breach/.

Identify what happened. Although some of the details regarding a data breach may have been ascertained in the hours immediately following detection of the incident, now is the time for the team to take a closer look at the details and develop a complete picture of what actually occurred before and during the event.

Cyberattacks and data breaches come in many varieties and from many sources. These include straightforward, unintentional errors on the part of employees and contractors, as well as coordinated, large-scale actions attributable to nation-states, organized hacking groups, and other threat actors. The following are some of the more common causes of data breaches:

- *Loss or theft of equipment.* Users may misplace a flash drive, laptop, smartphone, or one of many other types of computing or media devices. In some cases, such devices may be stolen from the user. These losses and thefts are typically not well thought out and focus on the device itself, not the information or software on the device. Incidents of this nature require action, but rarely on the scale required by a larger, more premeditated attack.

- *Use of external/removable media.* An attack can be executed from removable media or a peripheral device. For example, malicious code could begin its spread onto a system from an infected USB flash drive.

- *Attrition.* Attrition attacks are those that employ brute force methods to compromise, degrade, or destroy systems, networks, or services. Examples of such attacks include distributed denial-of-service ("DDoS") onslaughts intended to overwhelm, and thus impair or deny access by others to, a service or application, as well as large-scale attacks against an authentication mechanism such as passwords, CAPTCHAs, or digital signatures.

- *Websites and portals.* Attacks can be executed from a website or web-side application. Examples include cross-site scripting attacks used to steal credentials or redirect visitors to a site that exploits a browser vulnerability and installs malware.

- *Email-based impersonation.* An attack executed through an electronic message or attachment, such as a phishing (broad-based) or spear phishing (aimed at specific, high-value targets) campaign. Such communications purport to be from a trusted source and encourage the target to provide sensitive information or click links or attachments that install malware.

- *Improper usage.* Any incident resulting from violation of an organization's acceptable usage policies by an authorized user.

The incident response team and its outside partners should determine whether any countermeasures, such as encryption, were enabled before, during, or after the compromise occurred. Investigators should also attempt to identify the attackers and validate the host (*e.g.*, IP address) of the attack. Details about the attack can be cross-checked against incident databases that are collected, stored, and consolidated by outside groups and government agencies, or the company can check its own knowledge base or issue-tracking system. Monitoring known attacker communication channels also may help pinpoint the source.

It is important to determine the exact date and time of each stage of the attack. The response team should look into when the attack was launched, when the attackers penetrated system defenses, the duration of the attack, and whether the attackers withdrew "voluntarily" or were stopped by the organization's action.

Determine the scope of the breach. A thorough investigation must be launched to identify the full extent of the breach or theft, including the type, location, and volume of information that was exfiltrated or compromised.

Eradicate the breach and initiate recovery efforts. After containment, it is important that the company eradicate all disruptive components of the technology that was used to launch the attack. Such actions include deleting malware, disabling breached user accounts, and identifying and mitigating all exploited vulnerabilities. Indicators of a compromise ("IoCs"), such as network intrusion sensor alerts, antivirus software alerts, changes to auditing configurations recorded on a host log, records of multiple login attempts from an unknown remote system, and even deviations and variations from normal activity noticed by system, email, and network administrators, should be noted, maintained, and updated as necessary on a formal list.

If the company does not already utilize a computer monitoring system such as an endpoint detection and response tool ("EDR"), they can deploy one with assistance from their forensic investigators. The EDR will continuously scan the systems and remove malicious files that may be involved in a continuous attack. The response team can also set up alerts during an active investigation to notify them of threats to block.

Following eradication of compromised or disrupted technologies, administrators should restore systems to normal operations and confirm that they are functioning properly. Recovery actions may involve restoring systems from their most recent, clean backups where possible. In other cases, recovery may require rebuilding, from scratch, systems that have been too compromised or damaged to repair. Other recovery steps include replacing compromised files, installing patches, changing passwords, and tightening the network perimeter.

To make sure that recovered systems are not inadvertently reinfected with some or all of the parts of the malicious code used to launch and conduct the cyberattack, it is important to rely on forensic experts to identify and fully delete hacker tools. The forensics consultants can also help the internal team determine whether there are other security gaps or risks and take steps to address them.

IV. NOTIFY INDIVIDUALS AND GOVERNMENT AGENCIES, AS APPROPRIATE

Notification activities are fraught with legal jeopardy. While there is no overarching federal security breach notification law, certain types of breaches may invoke exceptions based on compliance with federal legislation such as the Breach Notification Rule of the Health Insurance Portability and Accountability Act (HIPAA)[19] or international legislation such as the EU's General Data Protection Regulation (GDPR).[20]

All 50 states, as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have passed some form of data security law that requires private and governmental entities to notify individuals of security breaches that involve PII.[21] These laws have specific requirements for reporting a breach to government authorities and parties affected by the breach. From jurisdiction to jurisdiction, however, the requirements of these laws often vary depending on the scope, specific facts, circumstances, and results of the breach, such as the number of compromised

[19] HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414.

[20] General Data Protection Regulation, art. 33, "Notification of a personal data breach to the supervisory authority" (Apr. 27, 2016), https://eur-lex.europa.eu/eli/reg/2016/679.

[21] *Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (July 17, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

records, the nature of the stolen or compromised information, and the industry affected. The timing and method of notifications also vary.

With guidance from legal counsel, the organization must develop a complete list of all individuals and entities that should be notified of the incident. This list should include those to whom a legally required notification must be made, as well as others who, from the standpoint of public relations and crisis communications, should also be notified. Recipients of such notifications may include customers, employees, media outlets, governmental agencies, and regulatory boards. Legal counsel can also assist in determining the content of the notifications, which may include descriptions and timing of the breach, recommended actions, and useful resources (such as contact information for the Federal Trade Commission ("FTC") or offices of state attorneys general).

The timing of such notifications is also crucial and is in most cases mandated by law. Mishandling of notifications can lead to severe consequences, including fines and other unbudgeted expenses.

Internally, an organization's upper management should be updated regularly on the status of the breach and the incident response team's containment and recovery efforts. Daily breach reports should be compiled and contain all relevant facts about the breach, as well as planned next steps and the resources needed to achieve specific solutions.

Certain contracts with vendors and customers may include specific notification obligations. All relevant contracts should be reviewed for such terms, and the incident response team should work with legal counsel to ensure that all requirements are met. Other business issues may also need to be taken into consideration, including upcoming or potential initiatives (including product

or service rollouts, marketing programs, and public-relations campaigns) that might be affected by the breach or breach-response efforts, or that might impede such efforts.

Finally, appropriate communication with law enforcement is mandatory, particularly where the nature or scope of the breach invokes specific legal and regulatory requirements. For example, if ransomware is involved in the breach and organizational leadership decides to pay the ransom, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") requires that law enforcement be notified first, or the payor may face civil penalties for sanctions violations. OFAC has taken this position under the theory that ransomware payments could be used to fund activities adverse to the national security and foreign policy objectives of the United States and further embolden threat actors to engage in future cyberattacks.[22] Any negotiations with or payments made to cyber criminals must be handled by an entity authorized to provide these services — at no time should business leaders engage with a threat actor without legal consultation.

V. CONDUCT POST-INCIDENT ANALYSES

[22] *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, U.S. DEPARTMENT OF THE TREASURY (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

According to the NIST, "One of the most important parts of incident response is also the most often omitted: learning and improving."[23] Following the conclusion of a data breach, the incident response team should prepare reports from each of the key members and hold a postmortem, a lessons-learned meeting with representatives from across the organization. This meeting should be used to review what occurred and what was done to intervene in the breach, assess the effectiveness of the intervention, and identify strategies for preventing and preparing for a future cyberattack. This meeting should be held in a timely manner, as every day of exposure increases the likelihood that an organization will be subject to another attack, particularly if the breach in question achieved some or all of the threat actors' goals.

The agenda for a post-incident meeting should include the following discussion items:

- A full review of the incident, identifying what happened and when.
- Performance of staff and management at key stages of the incident.
- Adherence to pre-established responsive procedures.
- Information needs, noting, in particular, data that was lacking and when it was obtained (if ever).
- Missteps, including actions that may have had a negative effect on the recovery effort.
- Quality, efficiency, and effectiveness of information sharing with other team members and outside organizations, including recommendations for improvement.

[23] *Computer Security Incident Handling Guide*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Aug. 2012), SP 800-61 Rev. 2, at 38, https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.

- Strategies and tactics that can prevent future incidents and help the incident response team perform more effectively.

- Threat indicators or attack precursors that should be monitored in the future.

- Costs associated with the incident.

- Resources or tools that should be obtained and implemented in order to detect, prevent, mitigate, and recover from future incidents.

A key area for review is evidence retention. If they do not already exist in the IRP, the company should establish policies for collecting evidence during and after an incident, and determine how long evidence from an incident should be retained. The following should be considered during the creation of such policies:

- Prosecution needs, including preservation of evidence to prosecute the attacker in a criminal or civil proceeding.

- Data retention, including determinations of the period for which incident data should be maintained following resolution (*e.g.*, the General Records Schedule of the U.S. National Archives and Records Administration specifies that incident-handling records should be kept for three years).[24]

[24] General Records Schedule 3.2 (Transmittal No. 26): Information Systems Security Records, U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (Sept. 2016), https://www.archives.gov/files/records-mgmt/grs/grs03-2.pdf.

- Costs, including expenses related to storing hard drives and removable media and maintaining functional computers that can access such data.

The search for a data breach resolution vendor should occur prior to a cyberattack, not after. However, it is never too late to begin the process of identifying and working with a partner to help manage potential fallout from a future breach. Organizations should contact pre-selected vendors and work with them to choose business services and protection products (*e.g.*, credit-monitoring services) for individuals affected by the breach. If the business or organization does not have an existing data breach resolution agreement in place, legal counsel should be obtained to help draw up vendor contracts. At all times, companies should avoid sending sensitive information to vendors that are supporting the breach recovery and management efforts, particularly where such information is not required for the vendor's activities.

As part of this lessons-learned review, attention should return to the IRP. The IRP should be reviewed to determine where it held up and where it was insufficient in dealing with the threat. Consider creating unique incident response playbooks for different types of threats, including wire fraud, ransomware, DDoS attacks, business email compromise, lost hardware or storage devices, and the like.

VI. COLLABORATE AND SHARE INFORMATION WITH KEY STAKEHOLDERS

As part of the IRP, companies should consider collaborating with law enforcement agencies, internet service providers, customers, and other key stakeholders. These stakeholders include other organizations within the company's industry. A successful data breach at one company may pave the way for subsequent attacks on similar businesses; where one company falls (or is hobbled), others are likely to follow. Working together to plan for potential attacks, even with businesses that otherwise compete for customers and market share, can help ensure that those

not directly involved in the incident are better prepared to defend themselves and the industry as a whole against a similar threat.

Given the sensitive nature of PII and proprietary data, as well as the vast web of data privacy and breach notification laws and regulations, organizations should consult with their internal legal departments or experienced outside counsel before initiating any coordination efforts with external advisors, forensic firms, and industry groups. Contracts or other agreements may need to be negotiated and put into place before such sharing begins.

Further, companies should share only necessary information with the appropriate parties. When sharing information with peer and/or partner organizations, incident response teams should communicate technical information (including external indicators such as the general characteristics of attacks and the identity of the attacking hosts) as opposed to business-impact information.

Information sharing should occur throughout the incident response life cycle, not only after an attack or breach has been resolved. This enables more effective coordination across the incident response team and helps coordinate defensive activities with organizations that may not be the immediate target of a cyber breach but could face a similar threat. Where possible, automated information sharing can improve efficiencies and support more cost-effective coordination.

VII. RISK MITIGATION STRATEGIES

The sheer breadth of activity required after a breach should prompt companies to promote preparedness and cyber defense. The strategies for those would fill another paper, but a short teaser is here. It is clear that cyber attackers take advantage of common exploits as well as the company's lack of cyber defense and preparedness. To help mitigate the risk of falling victim to ransomware

and other cyber-attacks and in an effort to better prepare for an incident, companies can take the following proactive measures:

- Protect your back-ups of critical systems – ensure that you have offline backups that cannot be impacted by an active threat on the network
- Design your networks, systems, and backups to reduce the impact of an incident – Ensure your privileged accounts are strictly controlled. Segment your network to reduce the spread of adversaries or malware. Have strong logging and alerting in place for better detection and evidence in the event of incident response. Having a technical security strategy that is informed by architects that know the latest attacks and adversary trends is important, as is the use of continuous threat intelligence monitoring in open source and on the dark web.
- Employ multi-factor or "two-step" authentication – Multi-factor authentication (e.g., a password – something employees know, plus an authentication key – something employees have) across all forms of login and access to email, remote desktops, external-facing or cloud-based systems and networks (e.g., payroll, time-tracing, client engagement) should be a requirement for all users.
- Install and properly configure EDR tools – Tools that focus on endpoint detection and response can help decrease the risk of a ransomware or other cyber attack and are useful as part of incident investigation and response. However, many entities that invest in these tools fail to properly configure them to be of assistance in the event of a cyber event and investigation. Properly configured security tools give a much greater chance of detecting, alerting on, and blocking threat actor behavior.

- Continuous Phishing Training - monitor and educate your users on phishing attacks, and ensure that cybersecurity awareness is an essential part of all job duties.

VIII. CONCLUSION

In today's information-dependent environment, cyberattacks and data breaches aren't just a threat; they are an inevitable part of doing business. However, with the right degree of planning and preparation, many such attacks can be prevented outright. Where attacks cannot be anticipated or prevented in whole or in part, an effective IRP and a well-coordinated team effort can minimize the damage, support rapid recovery, and help organizations maintain the favorable reputations they have worked so hard to foster with customers, shareholders, regulators, and other key stakeholders.