CROWDSTRIKE SERVICES

YOU’VE BEEN **BREACHED —** NOW WHAT?

HOW TO RESPOND TO A WORST-CASE CYBER SCENARIO

WWW.CROWDSTRIKE.COM

EXECUTIVE SUMMARY

Any organization with sensitive data can be attacked, regardless of size or industry sector. And as the threat landscape evolves and adversaries deploy tactics, techniques and procedures (TTPs), including destructive malware, ransomware and targeted phishing, security professionals and stakeholders must also adapt their security plans.

Depending on the situation, a targeted attack may involve the theft of source code, valuable intellectual property, negotiation data or general business disruption. Companies need to be prepared to identify, respond to and mitigate a targeted attack with the same amount of effort that goes into implementing a disaster recovery plan.

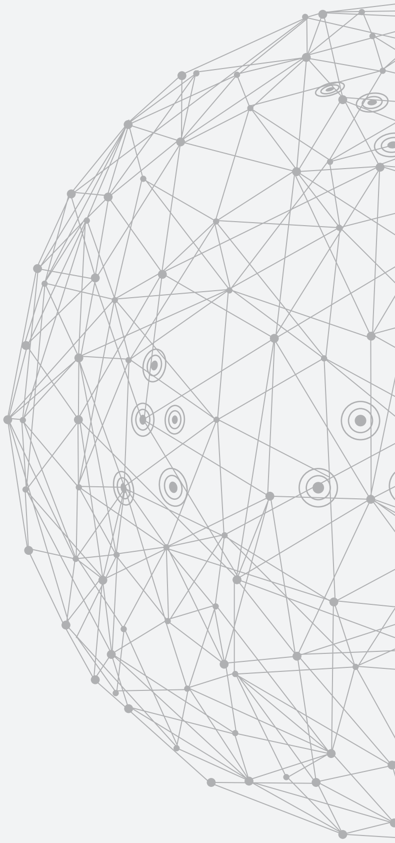
This document summarizes recommendations for responding to a breach and the expertise required to do so quickly and effectively. These recommendations were derived from decades of collective experience from the cybersecurity consultants at CrowdStrike®, who work on the front lines fighting threat actors every day.

THE AFTERMATH OF A BREACH

It's happened: You've received a breach notification — either from internal staff, an external tipster or law enforcement. Intruders have broken through your defenses and into your organization's environment.

What are your next steps? For C-level executives and front-line IT and security staff, there are two major sets of actions to take just after a cyberattack: short-term and long-term. In the short term, steps must be taken immediately to stop the bleeding of valuable data assets and preserve forensic evidence that will be useful during the investigation and remediation process. After you make it through a breach, you will need to take long-term actions to mitigate the risk of another breach.

All organizations should seek to proactively enhance their corporate information security procedures while avoiding common mistakes and pitfalls. The following recommendations can help your organization both prepare for and respond to the next targeted attack.



SHORT-TERM ACTIONS:

WHAT TO DO IMMEDIATELY AFTER AN ATTACK

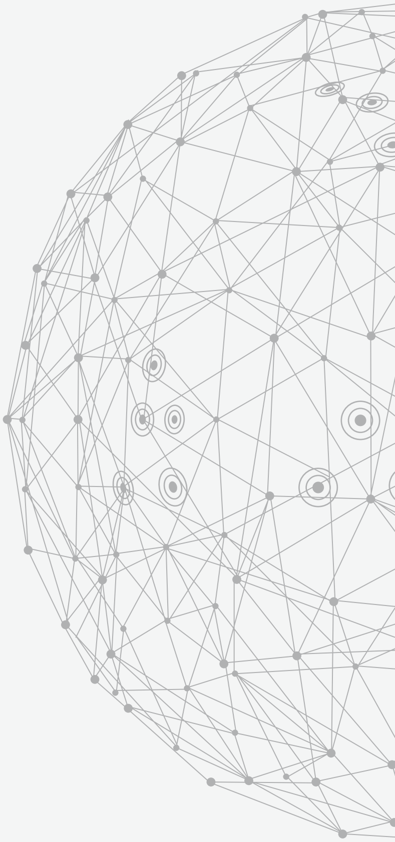
PRESERVE — COORDINATE — RESPOND

Cyberattacks are inevitable in organizations with sensitive data. When responding to these attacks, every detail is critical in protecting the business' reputation and preserving the customer's trust. The limited time to react during a breach requires that organizations have a well-thought-out and strategic approach that enables them to perform coordinated internal response efforts and swift decision making. To effectively react when notified of a breach, CrowdStrike believes your organization should concentrate on its ability to preserve, coordinate and respond.

PRESERVE

Do not disconnect

Many targeted data breaches go on for months before detection. When a compromised system is hastily disconnected, it is highly probable that the attacker will compromise additional systems to establish new forms of persistence that may go undetected, or they may have already prepared backdoors for these situations. Attacker behavior is likely to change, and a game of "whack-a-mole" may ensue once they know they have been detected. This is why the natural reaction of wanting to swiftly disconnect all affected systems can be counterproductive in the long term. If a computer must be disconnected, ensure that a forensic image



(including a memory image) of the system is preserved prior to disconnecting from the network.

Collect log data

Log data is often crucial in determining how the incident occurred, when the incident began, the range of systems affected and the data that was accessed or targeted. You must validate that all centralized host-based and network logs are being preserved, and that backups of critical servers are available. The incident may have started months before detection occurred, making all rolling logs valuable regardless of age. The attackers may also be quick to clear any unprotected logging if they feel they have been discovered.

COORDINATE

Establish internal communications

Formulating a response to a data breach requires internal communication and coordination within your organization. At a minimum, key players from IT, security, legal, management and public relations must be kept informed of the status of the data breach. Each player fulfills key functions that enable the investigation, the formulation of a response and the communication with regulatory agencies as well as customers. In some cases, if there is reason to believe internal network communications may be compromised, out-of-band communication and collaboration channels should be established and utilized by the response team.

Engage an incident response services company

Even large security teams often need "surge" assistance early in the incident response (IR) cycle and during remediation efforts. Establishing a retainer and getting initial paperwork in place can minimize delays to your investigative efforts when help is required. Companies that do not have a contractual relationship in place with an IR firm in advance of a breach typically take two to three times longer to get the support they need after discovery. Consider proactively partnering with a company like CrowdStrike that can provide the full range of services that will be needed in the short and long term. This will help ensure cohesive communication and planning throughout the entire process.

GET BACK TO BUSINESS FAST WITH CROWDSTRIKE

When a breach occurs, speed to remediation is critical. The CrowdStrike real-time incident response (IR) methodology provides advantages that traditional, slower IR approaches lack. With a comprehensive approach that ensures no threat goes undetected in your environment, CrowdStrike gets customers back to business faster and reduces costs by:

- **Providing accelerated time-to-visibility and remediation** with reduced forensic costs
- **Reducing business interruption losses** by getting you back to business faster
- **Minimizing cyberattack impact** by quickly identifying and ejecting attackers

TRADITIONAL IR APPROACH

MANY DAYS

- Ship servers
- Load software
- Fly consultants

WEEKS

- Run system scan (single snapshot)
- Analyze results
- Repeat until activity is seen

MONTHS

- Plug holes as they are found
- Rerun scans to look for more activity
- Analyze additional scans
- Repeat until consultant feels there is no more activity

CROWDSTRIKE IR APPROACH

HOURS

- Deploy CrowdStrike Falcon, cloud-based EDR

HOURS

- Conduct computer and human analysis of real-time activity

DAYS/WEEKS

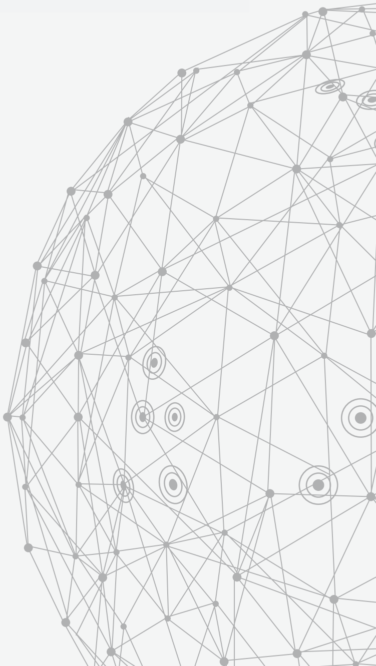
- Identify and contain adversary
- Remove adversary access
- Analyze forensic artifacts
- Plug holes

CROWDSTRIKE VALUE

- Reduce business interruption
- Gain greater visibility for better decision making
- Incur less expensive forensic engagement
- Reduce adversary impact

Understand legal requirements

For U.S. companies, the creation and enforcement of minimum notification standards currently is a state's rights issue. Forty-seven states as well as Washington D.C., Puerto Rico, Guam and the U.S. Virgin Islands have some form of data breach notice requirement. It is important to ensure your organization understands the requirements for all of the geographies and jurisdictions within which it operates.



RESPOND

Monitor workstations, servers and internet egress points

Legacy signature-based antivirus solutions typically cannot provide the real-time visibility across your endpoints necessary to detect and stop sophisticated attacks. An endpoint detection and response (EDR) solution provides the visibility that can be crucial in stopping targeted attacks before they can cause damage. Deploying a cloud-based EDR solution also accelerates recovery time after a cyberattack. You can ensure that damage is limited, data exfiltration has stopped and remediation can begin by leveraging an endpoint technology that enables your security staff to detect, prevent, record and search in real-time. Monitoring internet egress network traffic ensures enhanced coverage for unmanaged endpoints and provides additional context to an attack.

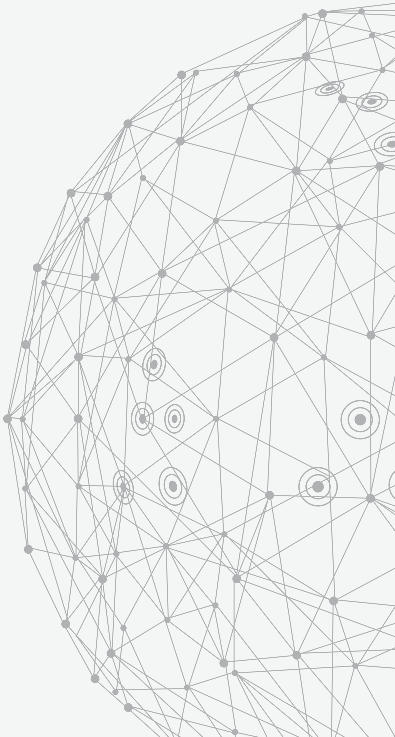
Scope and investigate the incident

Proper scoping of an incident during an investigation is critical to concentrating resources on containment and eradication efforts. Without an accurate scope, attackers may maintain their presence within an environment. Responders will need to conduct endpoint and network forensics to identify active malware in your environment, the source of attack and attacker attribution. Endpoint forensics will help determine how many systems have been accessed or compromised, what data may have been accessed, how long the incident has been occurring, the initial attack vector, persistence mechanisms in your

environment and exfiltrated data. If a credit cardholder data environment has been affected, you may need to bring in a PFI-certified forensic firm approved by the PCI Security Standards Council to investigate.

Remediate the attack

Remediation efforts should be coordinated in a way that completely removes the attacker from the environment and limits his ability to return in another way. Isolate critical systems (i.e., point-of-sale, CRM, inventory management) from the broader network and block access to the adversary's command and control infrastructure. Remove and completely refresh infected hosts. Perform credential resets where needed. Then, assess additional measures to harden the environment based on the findings of the incident response investigation and security review.



LONG-TERM PLANNING:
STOP THE NEXT BREACH

GOVERN — SECURE — OPERATE

Today's sophisticated attackers will not limit their tactics and techniques to known malware and exploits. Therefore, conventional malware-based protection is insufficient to stop targeted, persistent attacks. Careful consideration and long-term strategic planning should be devoted to preparing for these attacks. Address threats proactively under the pillars of govern, secure and operate.

GOVERN

Have a data breach response plan in place

A data breach plan should establish best practices, define key roles and responsibilities, and identify a process for the organization's response efforts. Plans should focus on internal efforts to restore data and systems' confidentiality, integrity and availability, as well as external requirements such as contacting insurance carriers, law enforcement, regulators, customers, vendors and public relations teams in response to the loss of potentially sensitive data. This is not just a paper exercise; an effective response plan requires that all parties involved understand their roles within the process, and it should include regular vetting and updating as people, process and technology changes occur.

Implement a cybersecurity risk management program

The identification, evaluation and prioritization of cybersecurity risks enables you to foresee issues and proactively determine appropriate responses. Decisions around planning and prioritizing security controls should be informed and supported by a mature cybersecurity risk management program.

Develop a cyber strategy and roadmap

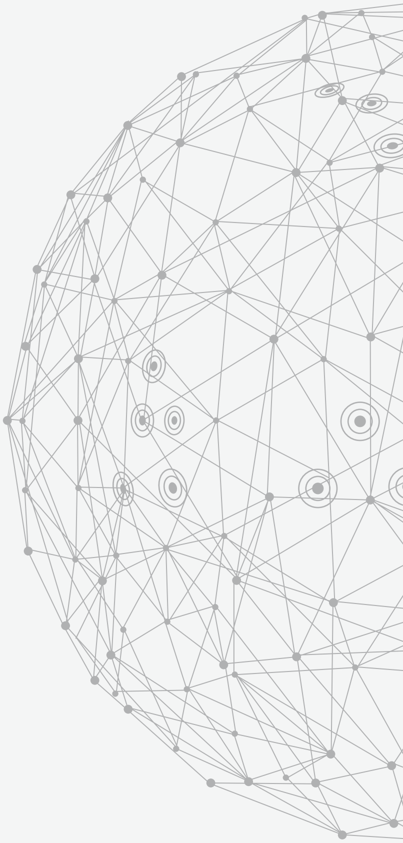
Once you understand the risks to your organization and the gaps within your cybersecurity defenses, set targets for maturity and goals to mitigate risk. These efforts should be prioritized along with your existing plans as part of a strategic roadmap for improving overall cybersecurity maturity.

Identify and classify assets

Organizations that try to protect all of their cyber assets equally often fail to protect what is most important to them. First, understand and then focus security controls on where the most critical and sensitive data and assets reside within your environment. This is essential to an effective cyberrisk mitigation strategy. This inventory should inform efforts to concentrate security resources and restrict access to your organization's most critical data.

Conduct regular education and awareness training

Educating your employees and increasing employee awareness should be part of your ongoing proactive security efforts. Your employees can become "human sensors" that identify and report potential incidents, such as a targeted spear-phishing or social



engineering campaigns. Employees throughout the organization should be aware of the importance of good security and know what to do if they suspect a breach.

Establish a metrics and reporting function

An organization cannot protect what it cannot measure. Therefore, cybersecurity controls and objectives should be continuously monitored and reported to key stakeholders. These metrics should be organized in a meaningful way to quantify risk and inform decision making. Regular metrics will give decision makers the ability to measure progress and set goals for improvement, as well as to prioritize security initiatives for maximizing return on investment.

Augment your IT team with scalable cybersecurity expertise and resources

We live in an age where cyber talent is hard to find and expensive to retain. Professional security consultants utilize the latest cyberthreat intelligence via feeds or other reporting sources. This enables them to access the latest threat actor tactics, tools and procedures (TTPs) which can inform their investigation of an incident. It also means these experts will have a greater ability to attribute a cyberattack to specific threat actors.

SECURE

Identify, isolate and log access to critical data

Focus your limited resources on those areas of the network that are most critical to your business. Determine where your most sensitive data or networks are located and implement increased logging and network monitoring. Actively monitor network access and conduct frequent log reviews.

Implement centralized logging

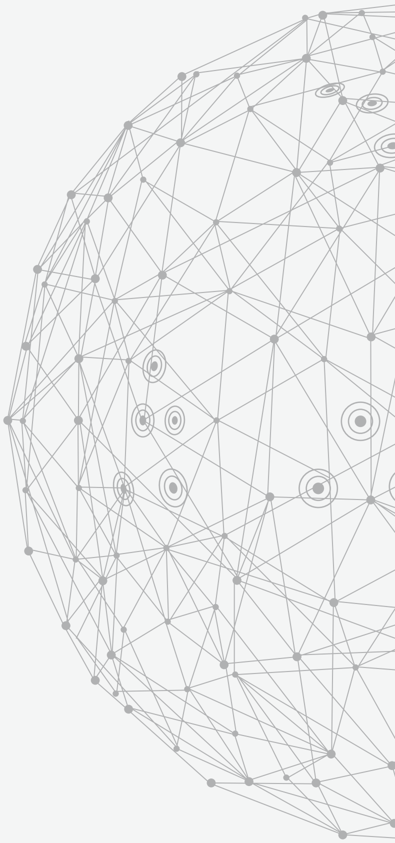
Having robust log aggregation and retention can support a data breach investigation by assisting responders in correlating certain events and developing an incident timeline. DHCP, DNS, Active Directory, server event logs, firewall logs, IDs and proxy logs should all be stored in a protected, centralized system that is time-synchronized and easily searchable. Allocate resources to perform regular log analysis and stress-test your logging process via tabletop intrusion exercises.

Consolidate internet egress points

In the event of an intrusion, monitoring egress points is also a critical part of identifying attacker activity. All connections to the internet from your corporate environment should be monitored to identify data leaving the network. The fewer egress points there are to monitor, the easier it is to detect malicious activity and the more cost-effective they are to monitor.

Apply operating system and third-party application updates

Patching operating systems and third-party applications is one of the most inexpensive, yet effective, ways to harden a network. It allows your employees to focus on detecting advanced adversaries. Build a strong patch management process and ensure that critical security patches are installed as soon as



possible. If you have legacy operating systems or software packages in your enterprise, develop and implement an upgrade plan.

Manage user credentials rigorously

Recent press coverage is littered with companies that did not adequately protect their user accounts. Passwords are consistently reported as being offered for sale on the darknet. If your organization maintains user accounts, audit your password storage functions. Solutions exist to make password management straightforward and secure by providing strong encryption and salted hashing, but they require proper implementation.

Keep a close eye on your Active Directory

Attackers use Active Directory configurations to identify attack paths and capture privileged credentials so they can deeply embed themselves into target networks. Most attacks today can be mitigated by securing key Active Directory components. CrowdStrike's Active Directory Security Assessment covers all of these components and more, and provides recommendations to help organizations secure their infrastructures.

Protect critical systems, including those outside your network perimeter

As the workforce becomes more mobile, centralized intrusion detection, file sandboxing and other security safeguards are not always capable of protecting all endpoint devices at all times. Advanced adversaries often deliberately compromise devices

outside your perimeter, taking advantage of the endemic poor security of other networks. Ensure that your endpoint solutions provide the same protection regardless of the location of the device.

Evaluate your cloud security posture

Cloud computing offers new possibilities and efficiencies for the enterprise as organizations migrate their applications to the cloud — both public and private. But innovation and reliance on the cloud introduces risk.

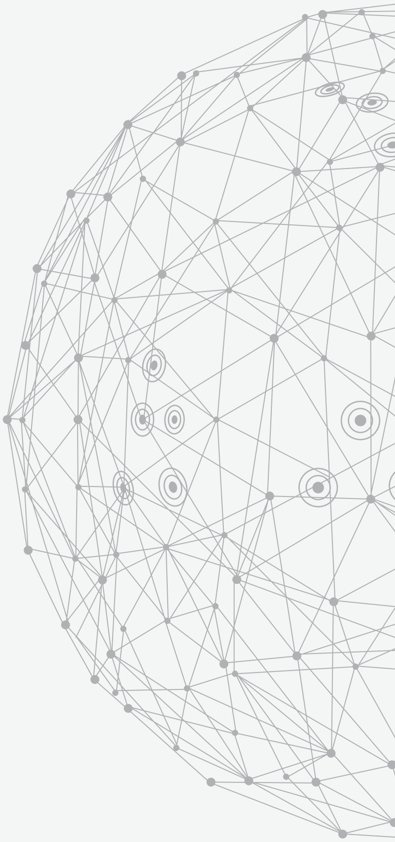
Therefore, you must continually assess your cloud infrastructure to determine if the appropriate levels of security and governance are implemented to counter these challenges. If not, CrowdStrike Services can provide recommendations for technology, processes and policies you can implement to improve your cloud security posture.

Require two-factor authentication (2FA) at login

Remote access into your network should always require two-factor authentication. Consider also requiring 2FA for sensitive administrative accounts. Out-of-band authentication methods such as SMS and soft tokens are commonplace, widely accepted by users, and relatively easy to implement with the prevalence of smartphones.

Change default passwords

One of the simplest attacks is to use a default password that is shipped out-of-the-box by a vendor. Internet of Things (IoT)



devices are commonly highlighted for this vulnerability, but the attack scope is much broader. Default passwords, especially for hardware devices (e.g., Wi-Fi routers), can allow direct access to critical data. Extra care should be taken to require strong passwords for all users, including default or built-in accounts.

OPERATE

Train like you fight

Testing IR readiness with tabletop exercises offers immense benefits when it comes to being operationally ready for a data breach. Working through roles, responsibilities and the steps of a complete IR plan prepares a team for action and quickly identifies any weaknesses in your plan, including processes, data collection efforts and team capabilities. This exercise may be helped by working alongside an IR services team with real-world expertise and up-to-date attack scenarios.

Training and educating your staff enhances and expands cybersecurity abilities. Consider classes on threat hunting to ensure a proactive approach to detecting intrusion attempts and activity. Teaching staff how to operationalize threat intelligence is also very valuable in establishing a proactive security stance.

Conduct regular red-teaming exercises

While still an integral part of an overall security program, simple vulnerability scans are not enough to evaluate your overall security position. Test your organization’s ability to stand up to the actual tools, techniques and procedures used by the

adversaries who actively target your industry. These exercises will give you a better understanding of your ability to prevent, detect and respond to targeted attacks.

Leverage cyberthreat intelligence

You cannot focus on all threats at once. Train responders to identify the most relevant threats by leveraging cyberthreat intelligence (CTI), which should be considered as important as other forms of business intelligence. Subscribe to vulnerability intelligence feeds and reporting, such as CrowdStrike Falcon Intelligence™, and ensure continuous monitoring via security platforms with the ability to automatically ingest intelligence data.

Encourage information sharing

Organizations that are better able to detect and respond to breaches often have integrated fraud and IT security departments. Encourage regular information sharing in your organization. IP addresses and system names associated with fraudulent transactions can be the indicators needed to identify other suspicious network activity or, ultimately, a data breach.

TAKE THE NEXT STEP: CREATE OR FORTIFY YOUR PLAN

CrowdStrike Services provides pre- and post-incident response services to proactively defend against and respond to cyber incidents. Both after and before a breach, the experienced team of cyber intelligence professionals, incident responders and malware researchers will help you respond to a breach, and prevent the next one. CrowdStrike Services has worked on some of the largest, most publicized and challenging intrusions and malware attacks in recent years.

CrowdStrike stops breaches. Call (888) 512-8906 or visit www.crowdstrike.com/services to learn more.

CROWDSTRIKE

crowdstrike.com

VER. 08.15.16