CYBER ATTACK SURVIVAL CHECKLIST

The Threat Landscape

Targeted attacks are inevitable in organizations with sensitive data. Depending on the situation, a targeted attack may involve the theft of source code, negotiation data, or general business disruption. Companies need to be prepared to identify, respond, and mitigate a targeted attack with the same amount of effort that goes into implementing a disaster recovery plan. From decades of experience, the consultants at CrowdStrike have created the following checklists to help organizations stop breaches before they occur by preparing for and responding to targeted attacks.

The unprecedented success of these attacks against large and well-equipped organizations around the world has led many security executives to question the efficacy of traditional layered defenses as their primary protection against targeted attacks. At the same time, many organizations have begun reviewing and revising their security best practices in advance of suffering a debilitating cyber attack.

Based on extensive use of CrowdStrike's next-generation endpoint protection platform to detect and prevent sophisticated attacks against large organizations, CrowdStrike's in-house team of security experts, adversary hunters, intelligence analysts and incident responders have pooled their knowledge to produce this valuable guidebook and checklist for proactively enhancing your corporate information security procedures while avoiding common mistakes and pitfalls.

Ver: 05-03-16

Cyber Attack Survival Checklist

Table of Contents:

Proactive Defense Checklist

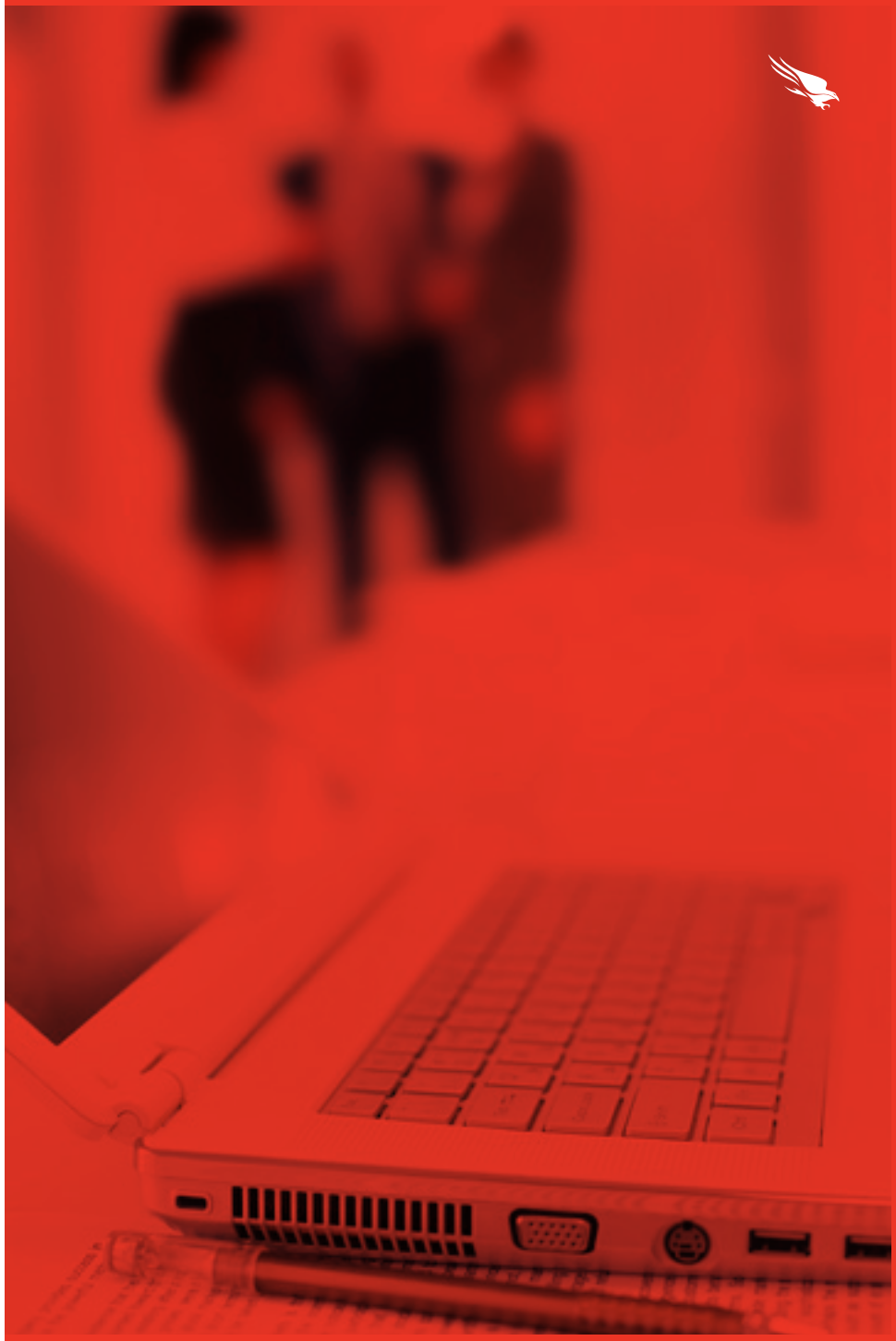
In an environment where 60 percent of attacks do not use any known malware, it is clear that conventional malware-based protection is insufficient to stop targeted, persistent attacks. CrowdStrike recommends the following steps to address threats proatively in this post-malware environment in which we operate today.

Gain Complete Visibility into Endpoint Data

Deploy cloud-based endpoint protection solutions to accelerate recovery time after a cyber attack. Ensure that damage is limited, data exfiltration has stopped, and remediation can begin by leveraging the full power provided by endpoint technology. The ability to access endpoint data allows for complete visibility into the full scope of an intrusion.

Consolidate and Monitor Internet Egress Points

In the event of an intrusion, monitoring egress points is 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 to monitor, the easier it is to detect malicious activity.



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

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.

Securing Web Applications and Internal Software Projects

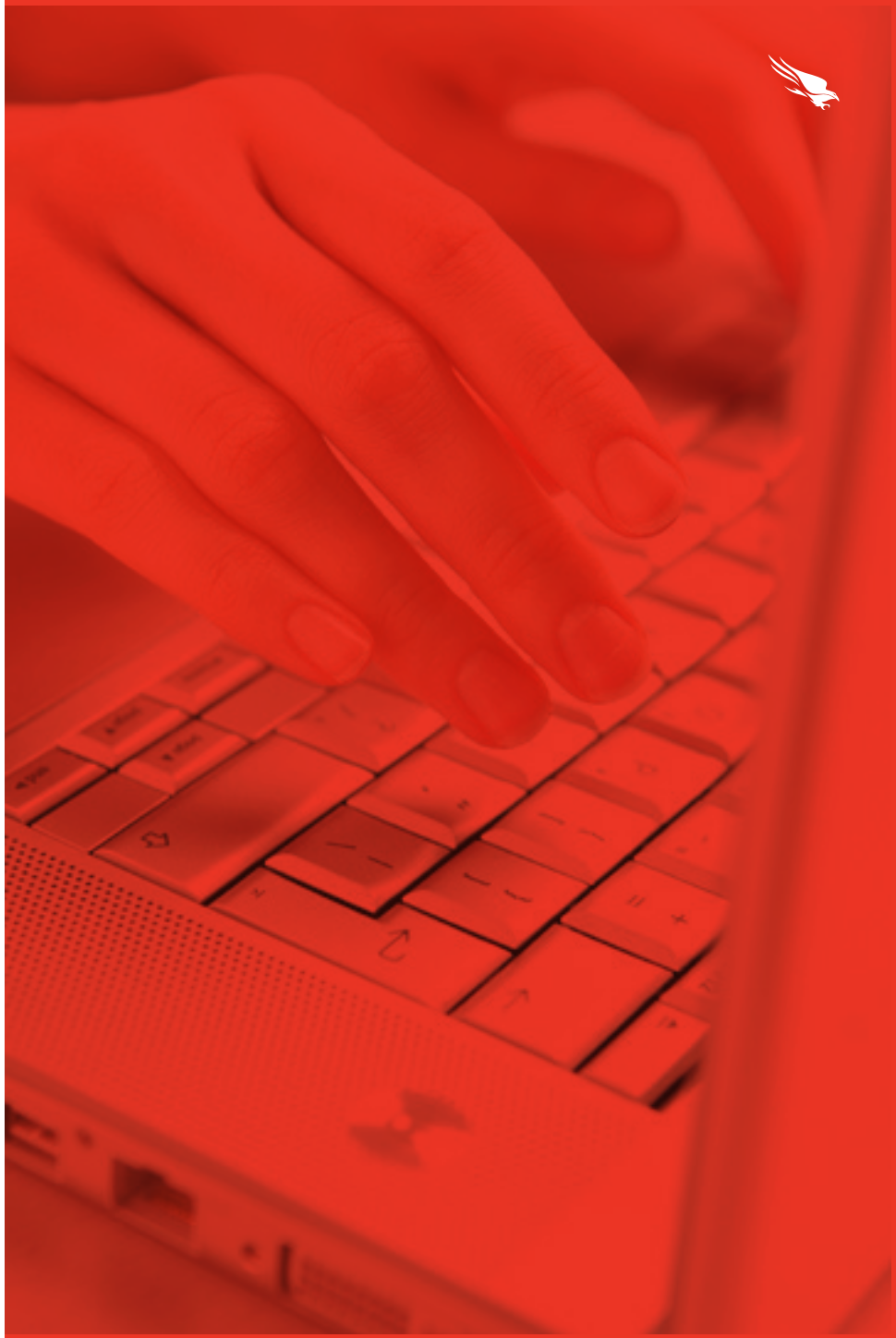
Web applications and homegrown software are regularly targeted and frequently compromised. Incorrect implementation of web application platforms can introduce vulnerabilities even on fully patched servers. Create a development culture focused on secure coding and conduct frequent

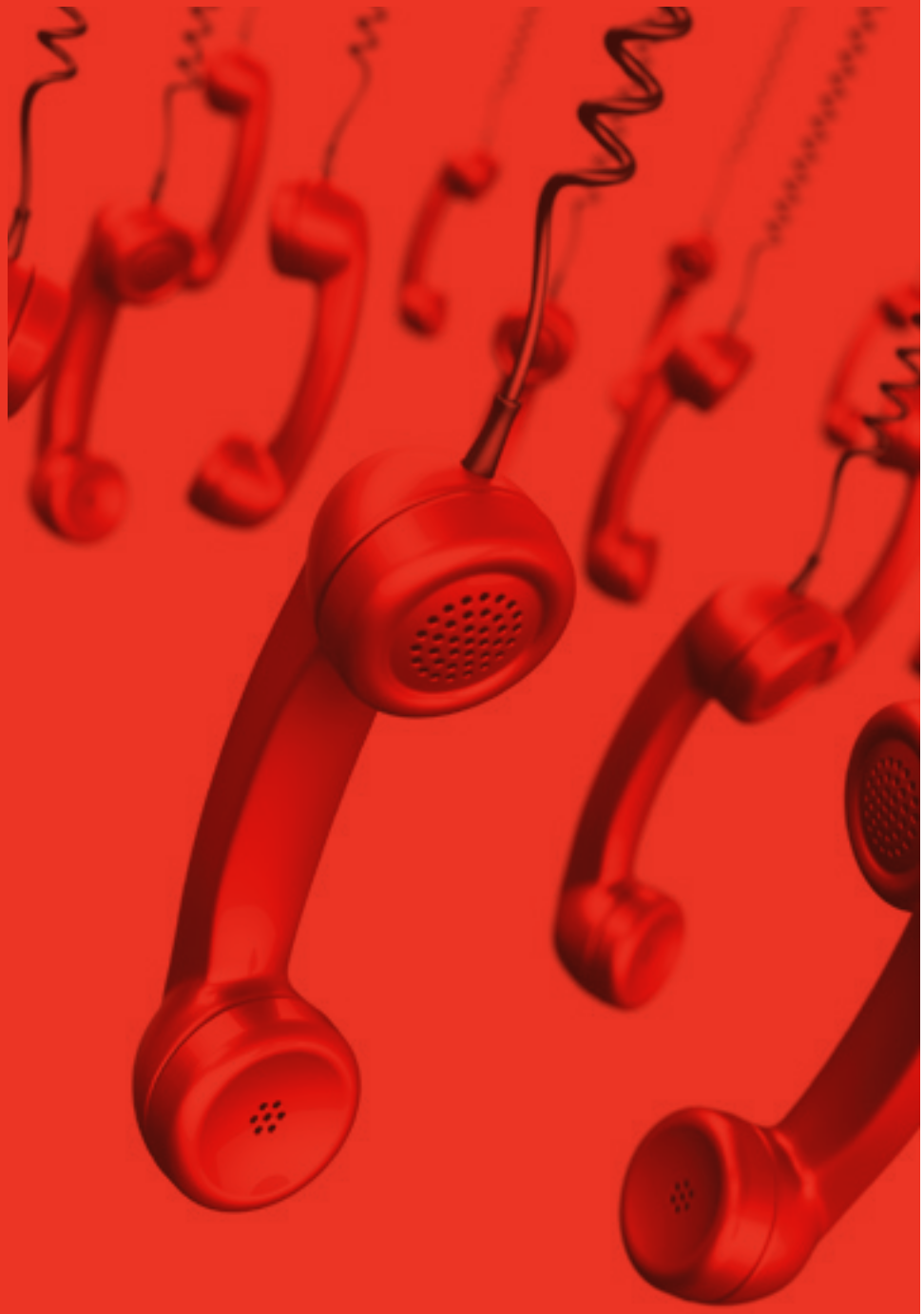
Patch, Patch, and Patch Again

Patching operating systems and third-party applications is one of the most inexpensive and effective ways to harden a network, while leaving your resources to be better spent on detecting advanced adversaries. Build a strong patch management process and ensure 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. Microsoft estimates that Windows 8 and server 2012 is six times more secure than Windows 7 and twenty-one times more secure than Windows XP.

Minimize or Remove Local Admin Privileges

Users should not utilize accounts with local administrator privileges as this opens multiple ways for targeted attackers to move laterally and compromise credentials. Disable the local administrator account on all workstations and servers via Active directory. If this is impossible within your environment, develop a password checkout procedure to ensure that every local admin account has a strong and unique password.





Implement a Tiered Active Directory Admin Mode

Use at least three levels of administration to isolate credentials and limit the damage due to compromise of critical accounts. A minimum implementation would be the creation of domain Admins, server Admins, and workstation Admins. No single account should be able to access all systems. Enhance logging and monitor the use of these privileged accounts.

Develop Incident Response and Data Breach Response Plans

Take active steps to prepare for a breach in advance. Incident response Plans tend to focus on efforts to restore data and systems' confidentiality, integrity, and availability. Data Breach Plans tend to focus on external requirements, to include for example contacting insurance carriers, law enforcement, regulators, customers, vendors, and public relations teams in response to the loss of personally identifiable information.

COMMON MISTAKES

Treating compliance as security

It is clearly a rational decision for organizations to focus on protecting data with regulatory scrutiny or requiring breach notification, and much of this oversight relates directly to the handling of personally identifiable information (PII). However, this data is rarely the only important information in your enterprise. Today's attackers can be just as interested in your intellectual property as they are in your customer's information. It all depends on which adversary you are facing. Good threat intelligence and counter-threat assessments can help you better understand your data risk.

Only protecting systems within 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 compromise devices outside of 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.

Single-Factor remote authentication

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

Storing account credentials with outdated hashing standards

The media is littered with companies that did not adequately protect their user accounts. If your organization maintains user accounts, audit your password storage functions. Well-known functions like pbkdf2 and bcrypt make password management straightforward, but they require proper implementation.

Not changing default passwords

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 passwordsfor all users, including default or built-in accounts.

Responding to an incident with an untrained team

Security/IT teams that are not intimately familiar with incident response may only uncover part of a compromise, lengthen an investigation, and leave a backdoor in place that allows the attackers to come right back into the enterprise. Incident responders must be well-trained, well resourced, and solely dedicated towards hunting for targeted attacks.

Not allocating money for security needs

The average data breach in 2013 cost $5.4 million. Many breaches could have been detected sooner or prevented entirely if analysts were alerted to anomalous or potentially malicious behaviors within their environment. A common mistake is to purchase new security solutions without budgeting for the human capital necessary to make use of them.

Not leveraging your security team to educate the masses

Spearphishing continues to top the list of initial attack vectors as users continue to click on suspicious links or open suspicious attachments. Basic security training and awareness for all employees can be very important to the overall security posture of the company. Use recent and relevant examples and do so regularly. Let employees know that everyone has a responsibility to protect the company.

STEPS FOR ENHANCING YOUR SECURITY TEAM

Train like you fight

Testing incident response readiness with tabletop exercises can be hugely beneficial. 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, processes, data collection efforts, and team capabilities. This exercise may be helped along by working with an IR services team with real-world expertise and up-to-date scenarios.

Education and awareness

Phishing attacks are still the most common attack vector. User awareness efforts and developing a network of human sensors can pay dividends.

Cyber intelligence feeds

You can't focus on all threats at once. Train responders to identify the most relevant threats by leveraging cyber threat intelligence. Cyber threat intelligence should be considered to be as important as other forms of business intelligence. Subscribe to vulnerability intelligence feeds 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 generally 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.

Have an incident response services retainer in place

Most breaches require the expertise and added manpower that come from an IR services team that faces these situations on a daily basis. A professional IR services team can greatly complement the capabilities of an in-house security/it team, while getting the answers needed on a timely basis and providing court-ready experience. 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 surge support they need.

RESPONDING TO A TARGETED ATTACK

Do not disconnect!

The majority of targeted attacks go on for months to years 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. If a computer must be disconnected, ensure that a forensic image (to include a memory image) of the system is preserved prior to disconnecting power.

Establish out-of-band communication channels

Assume that your network is completely compromised and the attacker can read email messages. Make phone calls, meet in person, and use email accounts not tied to the corporate email environment. Do not let them know you know, and do not let them know how you plan to fix it.

Contact an incident response services company

Even large security teams often need surge assistance early in the incident response cycle and during remediation efforts. Consider proactively identifying a service provider who can be available in case of emergencies. Establishing a retainer and getting initial paperwork in place can minimize delays to your investigative efforts when help is required.

Preserve all logs

Validate that all centralized host-based and network-based logs are being preserved and that backups of critical servers are being maintained. These logs may be crucial in determining how the incident occurred, when the incident began, the range of systems affected and the data that was accessed or targeted. The incident may have started over a year ago, making all rolling logs valuable regardless of age. The attacker may also be quick to clear any unprotected logging if they feel they have been discovered.

Scope and investigate the incident

Conduct network forensics to identify active malware in your environment, the source of attack, and attacker attribution. Conduct host forensics to determine how many systems have been accessed or compromised, which data may have been accessed, how long the incident has been occurring, the initial attack vector, persistence mechanisms in your environment, and exfiltrated data. Determine if a cardholder data environment has been affected.

Remediate the attack

Isolate critical systems (e.g. Point of sale) from the broader network. Block access to adversary command and control infrastructure. Remove and completely refresh infected hosts. Perform credential resets where needed. Assess additional measures to harden the environment based on findings of the incident response investigation and security review.

RESPONDING TO A TARGETED ATTACK

Report

Reporting requirements will vary based on the data accessed. As details become known throughout the course of the incident response investigation, prepare reporting per requirements and determine if media reporting is necessary. Prepare a FAQ resource or contact information for additional details.

Enable logging now

Logs of all kind prove invaluable during an incident response. However, it is often discovered duringan IR that logging was not enabled in many critical places, or that retention was very limited. Not only can logs help eliminate assumptions and provide faster tracking of an incident, their regular review may have detected a breach before it got off the ground, and certainly before it persisted for months.

Police and remove unused systems, services, software, accounts, and data

Dormant items in an enterprise are a major liability. They often fall under the radar of your patch management and administration efforts and can harbor significant vulnerabilities that are often targeted. The same is true for services, accounts, and miscellaneous data. It is not unusual for a company to update their security posture on a database, only to set aside the previously unprotected records for the taking. Regularly review system, software, and account inventories and purge those that are unused or not necessary.

WORKING WITH LAW ENFORCEMENT

WHO WILL YOU BE WORKING WITH?

Top-notch technical folks from the FBI or secret service. These two organizations are the most active in breach investigations within the United States.

WHAT WILL THEY WANT?

» Avoid tipping off the attacker
» Evidence collection and preservation
» Internal and external threat landscape specific to your company
» Investigative assistance
» When will it end?
» Weeks on-site, months off-site.

HOW DOES IT END?

Ideally, the combination of your company's internal vulnerability mitigation, detection efforts, and incident response along with meaningful law enforcement coordination stops the attack at its source.

WHY REPORT TO LAW ENFORCEMENT?

TOP 5 REASONS:

1 - Catching the bad guys is the surest way to get them out of your system.

2 - Apprehending the perpetrators also can result in the complete recovery of your data or otherwise minimize the harm of an intrusion.

3 - Working with law enforcement is more likely to helpfully inform your internal security efforts than to waylay them.

4 - If an intrusion results in the loss of personal data, law enforcement notification will likely be required, and depending on the status of the investigation, may allow for delaying a public notification.

5 - Reporting cybercrime provides government agencies with the data necessary to follow trends, calculate the impact of this growing problem, and ultimately lower your risk.

ABOUT CROWDSTRIKE

CrowdStrike provides next-generation endpoint protection, threat intelligence, 24-hour monitoring and incident response services to many of the world's largest and most advanced companies and government agencies. The 100% SaaS-based CrowdStrike Falcon Platform offers the most comprehensive endpoint protection technology available, enabling customers to detect, prevent, record and search in real time to stop targeted attacks before they can cause damage.

Request a demo of CrowdStrike Falcon and learn how to address today's most advanced threats with a true SaaS endpoint protection solution.

www.crowdstrike.com/request-a-demo

ABOUT CROWDSTRIKE SERVICES

CROWDSTRIKE SERVICES, a wholly owned subsidiary of CrowdStrike, Inc., provides pre and post Incident Response services to proactively defend against and respond to cyber incidents. CrowdStrike's seasoned team of Cyber Intelligence professionals, Incident Responders, and Malware Researchers consists of a number of internationally recognized authors, speakers, and experts who have worked on some of the most publicized and challenging intrusions and malware attacks in recent years. The CrowdStrike Services team leverages our Security Operations Center to monitor the full CrowdStrike Falcon Platform and provide cutting-edge advanced adversary intrusion detection services. The full spectrum of proactive and response services helps customers respond tactically as well as continually mature and strategically evolve Incident Response program capabilities. CrowdStrike Services is accredited by the NSA for Cyber Incident Response Services.

NEED IMMEDIATE ASSISTANCE?

TALK TO AN EXPERT NOW.

1.855.CROWD.IR (276.9347)

services@crowdstrike.com

CrowdStrike | 15440 Laguna Canyon Road, Suite 250, Irvine, CA 92618

WWW.CROWDSTRIKE.COM | @CROWSTRIKE