Guidance Software | Whitepaper

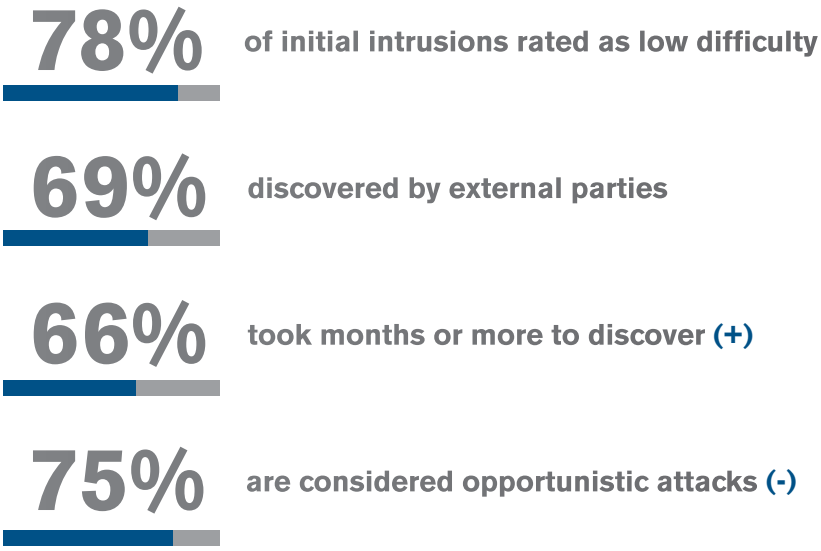
Incident Response: Six Steps for Managing Cyber Breaches

Guidance Software®

Introduction

Your network will be breached. This is a stark reality of the world in which we operate and do business. Each week brings new threats and reports of compromised networks and lost data. Like it or not, it is a simple fact that no organization is immune.

Consider this -- the *2013 Data Breach Investigations Report*, conducted by Verizon, found the following commonalities across 47,000 security incidents and 621 data breaches reported in 2012:



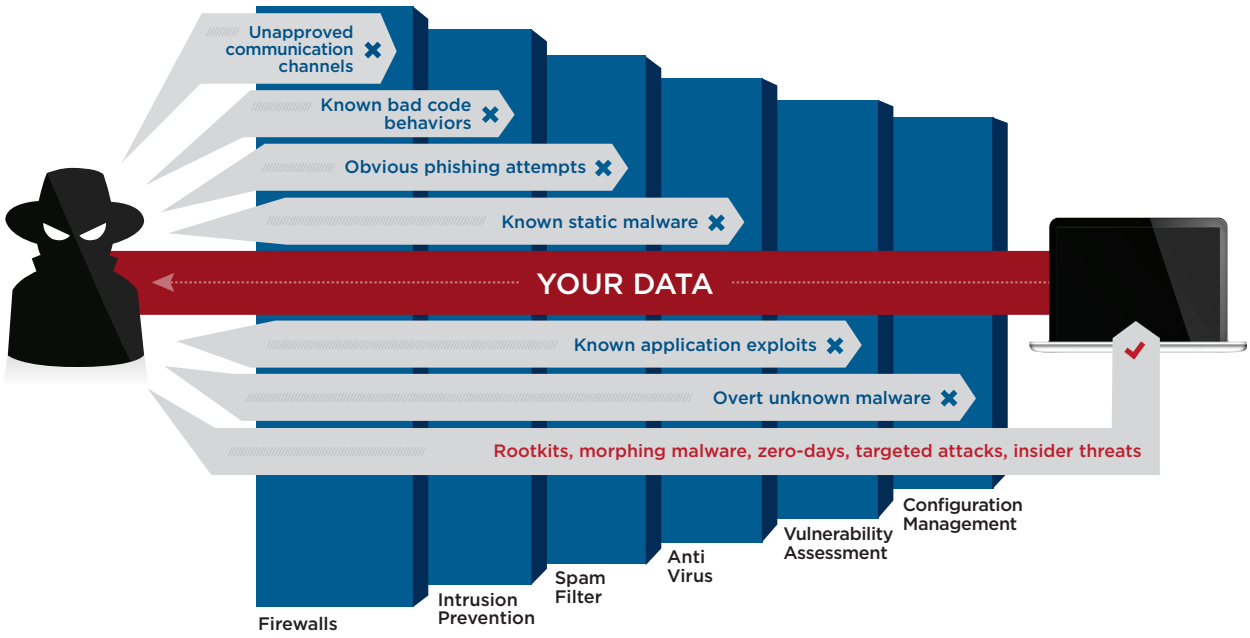
Source: Verizon, 2013 Data Breach Investigations Report

Your team's ability to quickly identify the breach, stop the exfiltration of data and classified material, and remediate real threats can have an enormous impact on your organization's risk, cost, and exposure. But when dealing with today's threats, staying on top of network security becomes increasingly challenging and putting in place best practices for managing cyber breaches can be the difference between containing an attack and letting it wreak havoc in your systems.

Key Information Security Challenges

The changing landscape of cyber security has brought new challenges to information security teams, including the undeniable facts that:

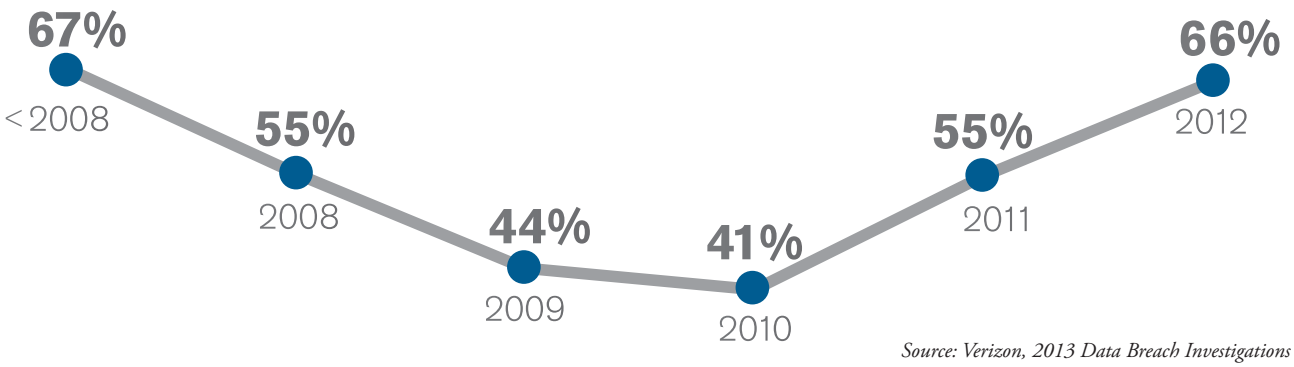
- **Perimeter defense is insufficient.**
  With new technologies come new exploits. Advanced threats like rootkits, morphing malware, zero-days, and insider threats are rarely caught by perimeter security solutions that rely on signature-based algorithms to detect known threats. But when the threat is constantly changing, brand new, or simply unknown to your perimeter security frontline, it goes undetected, much like when the infiltration is caused by an insider whose credentials give them access to your network or sensitive data. Today's cyber attackers will not be stopped at the perimeter. Many of them are already past your firewall, whether you have found them yet or not.



- **Attacks are becoming increasingly targeted.**
  At first, hacking was merely a pastime for computer-savvy individuals seeking to challenge their skill sets and knowledge. But those days are long over. While the majority of attacks are considered opportunistic – meaning the attacker did not intentionally target the victim -- nowadays, financial, espionage, and activism motives are driving the majority of targeted attacks. Malware is being custom-designed for specific targets, and hacking has even become "productized." Attack nets are not cast that widely anymore – instead, they have become increasingly targeted at people in certain roles, such as high-access executives toting tablets and laptops, or at organizations for their involvement or support of debated principles.

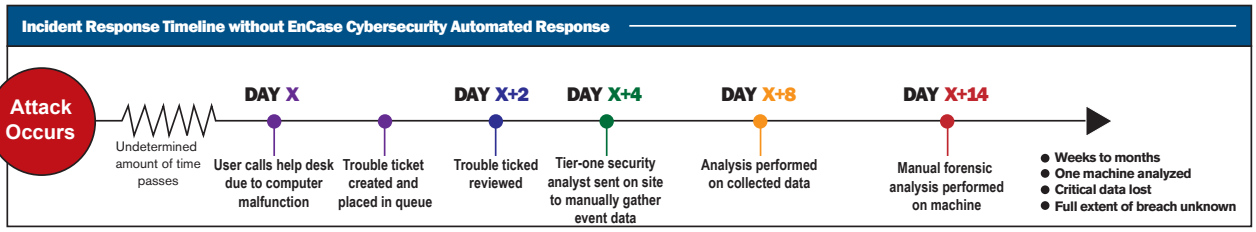
- **Threats are becoming harder to eradicate.**
  Cyber-attacks involving polymorphic malware or advanced persistent threats (APTs) are often extremely sophisticated due to the use of stealthy techniques, making it substantially more difficult to eliminate or remediate. Clearly, time is of the essence when such attacks take place. Depending on what type of alerting technology you have, it could be weeks or months before you know that any of these threats has turned into a successful breach.

Percent of breaches that remain undiscovered for months or more



Source: Verizon, 2013 Data Breach Investigations Report

- **Most organizations still respond manually to incidents.**
  Despite being bombarded with numerous attack attempts on a daily basis, only a few organizations have network-enabled incident response processes in place. The traditional manual process is incredibly slow, and typically begins with a call to the help desk sounding the alarm, the generation of a trouble ticket, and then event correlation or a security information and event management (SIEM) analysis. The challenge is that this manual process can take days, weeks, even months, which is simply untenable when further damage may be done during the painstaking response process.



The reality is that when it comes to cyber-attacks, defenders have to be right 100 percent of the time to avoid being breached, while hackers only have to be right once to succeed. A determined hacker will find a way to achieve his or her agenda.

Six Steps for Managing Cyber Breaches

Operating under the assumption that a security breach is practically unavoidable, organizations must adopt new postures to be prepared for and successfully respond to incidents right at the first sign of intrusion. The following six steps are intended to guide organizations in properly managing cyber breaches.

Step #1: Preparation

The more prepared you are to act immediately – and with some degree of automation – the better. Since the first part of preparation is always training of team members—and some part of that should be done for all employees—make that "job one" and be sure that training covers:

- Incident response processs planning
- Tools and trends
- Security awareness

Many government agencies and enterprise organizations take security-awareness training seriously. For example, unsatisfied with a 95% compliance rate, in 2012 the Veterans Administration created a policy that temporarily "unplugs" from the network those employees and contractors who skip their yearly cybersecurity refresher courses.

Test Your Processes

To prepare your processes and train your team, map out five or six different scenarios involving different variants of methods by which your network could be breached. These are called "tabletop exercises." Bring in key people from human resources (HR), communications, system administration, information security, legal, compliance and auditing, and network communications and discuss how their different business units come into play when you go through each scenario.

The widely varying responses to the question of what each is supposed to do can be surprising. System administrators will often say, "Well, we'll just format the box." In some cases that is the right answer, but in others, that may not be the best solution because your legal team, HR department, and possibly the FBI could request that the infected system be put in a quarantined containment zone for observation of malware behavior. This can be instructive in learning where the malware is connecting or "phoning home" to so that a wiretap can be placed on that number.

The time to meet with your team to discuss how you are going to handle a breach should never be when your first big breach has already taken place. Advance planning and training are critical.

Perform a Proactive Sensitive-Data Audit
Know where sensitive data resides as early as possible and come up with a data protection strategy. These measures can save you countless hours of inventory that would have to be done in the heat of the moment after a cyber-attack. Perform a complete inventory of all sensitive data in your organization, including:

- Personally identifying information such as credit-card data
- Intellectual property
- Classified materials
- Any data under regulatory or compliance control

Process Maintenance
To make sure that your team is always ready and up-to-date, you should:

- Understand sensitive data location and use
- Keep systems patched and up-to-date
- Conduct ongoing vulnerability testing
- Implement full incident response process
- Continually test and refine the process with regular "fire drills."

Step #2: Detect and Expose

It is estimated that over half a million attacks barrage government agencies and *Fortune 500* companies on a daily basis. Unfortunately, no SIEM system is ever tuned to such a fine degree of precision that only the critical situations that need attention are immediately presented to the incident response team. Two ways to proactively and effectively validate cyber threats are endpoint security analytics and security automation.

Endpoint Security Analytics
Leveraging data from across all your servers and end-user devices – including running processes, connections, machine names and IP addresses, and other valuable data – endpoint security analytics give you complete visibility of your network's activities, allowing you to detect anomalous behavior, risks areas, and security threats before damage can be done.

Security Automation
Integrating network-enabled cyber forensics tools with your SIEM systems helps you quickly reveal and validate suspect or mutating software on any endpoint in your network. Your cyber forensics tool should be able to work across platforms, and do so quickly, as speed is essential to finding and collecting actionable volatile data.

Step #3: Triage

Once you have identified that you have a problem, your next steps are to:

- Scope the threat to understand the extent of the compromise and its ongoing capabilities
- Zero in on the biggest threats first, and
- Determine whether personally identifying information (PII) and / or intellectual property (IP) was compromised.

This is where your proactive sensitive data auditing against a predefined baseline of where your data is and should be stored can save you significant time. With the data map in hand, you are two giant steps closer to knowing which data was the likely target of the malware.

The ability to scope the threat is also a tremendous advantage. Many companies make crucial mistakes in this area by overestimating the degree of exposure of the breach to the organization. This can result in negative customer or brand impact that can be completely avoidable.

For example, under PCI DSS (Payment Card Industry Data Security Standards) regulations, if an organization accepts credit-card payments and is the victim of a breach, they are required to notify federal authorities about the incident. But if an analysis of the breach reflects that internal credit-card numbers stored on the network were not compromised, the company is not required to issue a public statement for state and federal agencies which could have otherwise damaged the company's reputation as well as its patronage from customers.

Understanding what has happened, which and how much sensitive data has been exposed, what the issues are, and how to remediate quickly are indispensable capabilities.

Step #4: Classify and Contain

During this stage the focus should be on enabling both short-term and long-term containment of the threat's progress into your enterprise environment. At this point, you will typically bring in a forensics team – in-house or outsourced – that can handle malware with reverse-engineering capabilities.

The major goal of the containment phase is to determine how to eradicate malware off the network. Many incident response teams create a sandbox to observe the malware and understand what it does and how it behaves, which will help in determining the best way to contain it.

As part of the analysis, the forensics team will:

- Remotely collect malware and relevant data with network-enabled forensic tools
- Collect and preserve volatile data as potential evidence
- Capture the crucial malware and artifacts
  - Determine whether it is polymorphic or metamorphic
  - Discover hash values and registry values
- Recommend remediation steps.

Step #5: Remediate

Now that you have identified what the malware is, what it does, its characteristics and hash values, as well as which and how much sensitive data has been breached, it is time to remediate.

Your incident response team can begin remediating systems by deleting all malicious or unauthorized code (*if appropriate*), both on the identified or target systems, and then proactively, network-wide. At this time, they should also conduct a post-attack sensitive-data audit of the affected machines to ensure data resides only where it safely belongs in your network.

Once the incident has been remediated, continuous monitoring of your network's activities will be instrumental in determining whether or not the remediation steps taken were sufficient to successfully return systems to their original, optimal state.

Step #6: Report and Post-Mortem

At this point, your incident response team should consult relevant data breach-notification regulations and policies for each of the industries in which your organization does business. Your legal, IT, public relations, and executive teams should have a breach-notification plan in place and be ready to take the appropriate steps when you present your incident report to them.

Your report will be vital to all concerned with business reputation, viability, and operations. It is highly advisable to be as clear and non-technical as possible in your reporting. If your report cannot be understood by key stakeholders, the value you are contributing will not be recognized.

Be sure to include a sunset or post-mortem report, which is a list of lessons learned from the incident, including:

- What the organization intended or planned to do
- What went right
- What went wrong
- What can be improved upon.

Consider modifying existing incident response plans and/or company policies to reflect any lessons learned from each cyber breach.

Conclusion

Information security breaches are inevitable, and the sooner your organization adopts a posture based on this assumption, the more prepared it will be to contain and remediate the damage they may cause. The speed at which you identify the breach, halt progress of infectious malware, stop access and exfiltration of sensitive data, and remediate the threat will make significant difference in controlling risk, costs, and exposure during an incident. Knowing these six essential steps to incident response can greatly increase your success in managing a cyber breach.

Our Customers

Guidance Software customers are corporations and government agencies in a wide variety of industries, such as financial and insurance services, technology, defense contracting, pharmaceutical, manufacturing and retail. Representative customers include Allstate, Chevron, FBI, Ford, General Electric, Honeywell, NATO, Northrop Grumman, Pfizer, SEC, UnitedHealth Group, and Viacom.

About Guidance Software (NASDAQ: GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® Enterprise platform is used by numerous government agencies, more than 65 percent of the *Fortune 100*, and more than 40 percent of the *Fortune 500*, to conduct digital investigations of servers, laptops, desktops, and mobile devices. Built on the EnCase Enterprise platform are market-leading electronic discovery and cyber security solutions, EnCase® eDiscovery and EnCase® Cybersecurity, which enable organizations to respond to litigation discovery requests, proactively perform data discovery for compliance purposes, and conduct speedy and thorough security incident response. For more information about Guidance Software, visit www.encase.com.

For more information about Guidance Software, visit www.encase.com.