GreyCastle security

WHITEPAPER

YOU'VE BEEN HACKED – NOW WHAT?

EFFECTIVE INCIDENT RESPONSE PROGRAM

TABLE OF CONTENTS

INTRODUCTION

Why an Incident Response Plan is Essential

Alarming results have been announced following a recent survey conducted by the Ponemon Research Institute and Juniper Networks. In their survey, 583 American companies were interviewed on security related questions. The result seems to correlate with what we have been seeing in the media during the past year; hackers are nearly always successful in their endeavors to break into your company website, and stopping them is no easy task.

The headline figure shows that 90% of companies suffered a computer hack in the past 12 months alone. More often than not, companies are actually suffering from multiple successful attacks from hackers. 77% of the companies that were successfully attacked were actually hacked multiple times. The question is no longer if or when you'll get breached, but how often and how impactful a breach will be.

WHY WE'RE VULNERABLE

Business Complexity

Was Target negligent or did they just have too many noisy alerts to chase? What does that mean? Here's an analogy that may help make sense of it. I'm sure you've seen shoplifting sensors at the front doors of nearly every retail store. What happens when they go off? Does the store guard rush forward and tackle the shopper? Do the cashiers holler for help? Do iron bars descend to block the exit? The truth is nothing happens because the alarms beep all the time. Everyone in the store, including the store personnel and other shoppers, have learned to tune them out because 99.9% of the time they mean absolutely nothing. Now step back and consider an organization the size of Target. They have more than 360,000 employees worldwide, about 2,000 stores, 37 distribution centers and a heavily trafficked retail web site. Their network is massive. A network that size may issue up to hundreds of thousands of alerts a day.

Economics

In many cases, cybercriminals have two choices: be poor and bag groceries for minimum wage, or be a cybercriminal who exploits Americans and buy luxury cars for everyone in your family. Cybercrime is not illegal in many countries and is actually encouraged or even state sponsored. If you're an American business, you are 10x more likely to be attacked.

Politics

International law does not allow for prosecution of cybercriminals between countries such as the US and Russia, so many times it's a fight that cannot be won.

Security Feelings Do Not Match Reality

Why do we keep buying antivirus? Not because it works, but because it makes us feel better. Human beings are programmed to ask the wrong questions – How secure am I? Am I more secure than my neighbor? We love this metric but it's meaningless because your neighbor is a mess. This is driven by the need to feel more secure. However, the feeling is irrelevant.

The real question should be, was the investment in security worth it? Risk management helps us separate feelings from reality. With antivirus being less than 30% effective on average, the question becomes is it making us more secure or simply more comfortable?

DEVELOP YOUR INCIDENT RESPONSE PLAN (IRD)

Asking the Right Questions

In order to know where you're going, you first need to know where you are.

- Does your organization have an Incident Response Plan?
- If you have a plan, has it been tested?
- If you have tested your plan, will it be effective?
- Does your plan include the right representation?

Planning for Failure

According to the National Institute of Standards and Technology (NIST) there are four stages in the incident response life cycle.

- **Preparation** – You need to build a plan and test it.
- **Detection and Analysis** – People can be a great monitoring system, but can you triage?
- **Containment, Eradication and Recovery** – Once we understand can we contain the damage to both operations and reputation?
- **Post-incident Activity** – We always learn something new from every incident.

DEFINE YOUR INCIDENT RESPONSE MANAGEMENT TEAM

Incident Management vs. Incident Response

When it comes to defining your Incident Management Team, there are key areas, questions and individuals that play an important role in managing an incident.

- **Lines of Business** - Such as corporate owners; help identify important business assets and drive process improvements.
- **External Investigators** – Who will hire in each potential situation? How quickly will they respond and how much will it cost?
- **IT** – Find out who owns and manages each system. Who has forensics skills? Who has database administrator access?
- **Corporate Communications** – Who is responsible for conveying relevant messages to employees, partners, or customers? Who will craft and approve that message to ensure that it is correct?

Building Your Team

When you show up on-site it's like someone giving you the pieces to a puzzle without the picture. You've got to start piecing things together analytically and figure out the details that paint the picture. You can't do this without your IR team.

So how do you build an incident response team? Just like the Navy SEALS, the best IR resources are born not made, so find them! Next you need to train and test them. Even good resources need practice and won't always know what to do. Finally, locate them near incidents. If most incidents happen in a particular area, then put the IR team there.

TRIAGE

Critical Factors

The name triage comes from a French medical term, which describes a situation in which you have limited resources and have to decide on the priorities of your actions based on the severity of a particular case. In the incident response handling process, the triage phase consists of three sub-phases: verification, initial classification and assignment.

Every organization should be asking these questions when performing triage:

- What is the impact?
- Is there collateral damage?
- How many people do you need to handle this incident?
- Which incident handler should be appointed to the incident?

FORENSICS

Critical Factors

It sounds cool, but it's a very difficult process to get it right. Your forensic plan will depend highly on what you're trying to accomplish – from a legal perspective, from a breach notification perspective. Going to litigate? Are we going to get attorneys involved – reporting, internal employee investigation? If there is going to be some type of litigation, forensics goes into hyper mode. If not, then we'll switch our efforts to recovery.

Authorization before investigation? If retaining an outside organization, use an attorney for that contract so that it's all privileged information. Make sure you're logging and establishing secure storage locations. Finally, leave it to the experts. If you don't know what you're doing, don't do anything.

INVESTIGATION

Critical Factors

The first step in investigation is to know your Indicators of Compromise (IoC). This includes outbound traffic, suspicious activity, large data transfers, strange logins and use of logins. Preserving evidence correctly is critical in an investigation. Everything from chain of custody to evidence bags, to secure storage must be done properly. Finally, prepare for the unexpected. Chances are there's much more to the incident than what is on the surface.

DATA BREACH REPORTING

Understand Your Reporting Requirements

Almost every U.S. state requires breach notification. In the U.S., 46 states plus the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. In fact, California recently updated their breach notification requirements to include notifying the State Attorney General when a breach affects more than 500 residents as well as adding new content requirements for breach notification letters.

Some U.S. Federal Law requires breach notification. The U.S. HITECH Act requires healthcare providers and other Health Insurance Portability and Accountability Act (HIPAA) entities to notify when a breach affects more than 500 individuals. Failure to notify individuals of a data breach could result in HIPAA violation and a fine of up to $50,000 per violation.

The PCI Data Security Standard provides very specific guidance on incident response. Requirement 12.9 states "Implement an incident response plan. Be prepared to respond immediately to a system breach." Requirement 10.2 requires "automated audit trails for all system components to reconstruct" seven categories of events. Appendix 1.4 requires an organization to "enable process to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider."

EXPOSURE OR BREACH?

Understanding the Difference

As incident response experts, we determine exposure. We can tell you if your information has been found on a carding forum, what's there, what it may mean, how it may have gotten there. We can tell you if your data has been exfiltrated and if your private information has been compromised.

However, we cannot tell you if you've been breached – only your attorney can do that. We must work with an attorney and provide data to help them make their decision. Has there been a breach and is it reportable?

TESTING AND TRAINING

Tips

As we all know, people can be your biggest asset or your biggest weakness. Testing and training is a cybersecurity effort that can't be overlooked. If you don't test, your plan isn't prepared and if you don't train, your people aren't prepared. In order to be effective, training should be early and often and a proper budget should be in place ahead of time.

RETALIATION

Do Not Hack Back

It's like going to steal the guy's car who just stole your car. He doesn't have a car, that's why he stole yours. Retaliation will do you no good in the best case and it will get you jail time in the worst case.

LESSONS LEARNED

Legal

- Be prepared to be sued – by clients, partners, vendors and everyone else.
- Allow your legal team to drive data retention and destruction requirements.
- Cyber laws differ by state so understanding your state's laws is important.

Insurance

Insurance can be confusing, so understanding what's required of you and what your policy covers is extremely important. If you lie on your assessment, you will not likely be covered. Insurance agencies will request copies of your IR plans, Risk Assessments, Tabletop Exercises and other cybersecurity efforts and if you can't produce the documentation, you probably won't get paid.

- Understand Cyber Liability Insurance – what it is and what it isn't.
- You may not get a policy without a cybersecurity program.
- Your breach may not be covered if the carrier deems you negligent to perform reasonably duty.

Information Technology (IT)

Your IT guys are not forensics experts or investigators. Just shutting down a computer or moving a mouse could compromise valuable information. If you think you're being breached don't do anything but pull the network cable, because it probably messes with the data.

Public Relations

Have you ever gotten a notification about a breach and what's being done and how they're going to fix it? Public relations and crisis communications plays a critical role in incident response, because the wrong message can do just as much damage as the original hack.

You need to know what to say, who needs to say it and when to say it. Different audiences such as media, customers and executives should be handled differently so having templates can save you time, money and energy when dealing with a stressful situation. Developing communications templates can also help you handle reporters, information leaks and other hurdles that could potentially tarnish your reputation.

If you don't tell your story, someone else probably will. Being as transparent as possible can many times work in your favor and minimize the impact.

LESSONS IS SUCCESS

The Key to Incident Response

Based on the hundreds of various types of incidents we have responded to, the one consistency is the importance of having an incident response plan. A fully documented, tested and trained plan dramatically reduced the response and recovery time.

The breach has become a positive training tool and preparation is key. Security is hard and incidents will happen, but having a plan will increase the efficiency and effectiveness of your response capabilities.

INCIDENT RESPONSE RESOURCES

Standards in Incident Response

- NIST Computer Security Incident Handling Guide
  http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
- US-CERT Handbook for Computer Security Incident Response Teams (CSIRTs)
  www.cert.org/archive/pdf/csirt-handbook.pdf
- ENISA Incident Handling Process
  http://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process
- HIPAA HITECH Breach Notification Rule
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/
- FTC Safeguards Rule
  http://business.ftc.gov/documents/bus59-information-compromise-and-risk-id-theft-guidance-your-business
- Internet Crime Complaint Center – www.ic3.gov
- Federal Bureau of Investigation – www.fbi.gov
- Information Sharing and Analysis Center(s)
- MS-ISAC, IT-ISAC, NH-ISAC, FS-ISAC, and others
- Local / State Police – 911

FOR MORE INFORMATION ABOUT GREYCASTLE SECURITY AND ITS CAPABILITIES

GreyCastle security

www.greycastlesecurity.com
518.274.7233
intel@greycastlesecurity.com