

Notifying LAW ENFORCEMENT

CONTACT LAW ENFORCEMENT AS SOON AS PRACTICAL SO AVAILABLE LEADS CAN BE FOLLOWED UP QUICKLY.

INTERNET CRIME COMPLAINT CENTER (IC3)

<http://www.ic3.gov/complaint>

Partnership between the FBI, National White Collar Crime Center and the Bureau of Justice Assistance.

Accepts online Internet crime complaints from actual victims or third parties to the complainant.

LOCAL AUTHORITIES (POLICE OR FBI)

<http://www.fbi.gov/contact-us/field>

Local authorities should always be your first point of contact. Many communities have cyber crime units (check listings).

A TRUSTED IT SECURITY CONSULTANT

We recommend reaching out to a professional cybersecurity specialist with credentials like a CISSP certification. Local universities may be able to assist as well.

YOUR LAWYER

Ensure your attorney is familiar with cyber regulations and policies. Areas like PCI, Sarbanes-Oxley, and HIPPA usually require specific knowledge and legal assistance.

Do Small and Medium Businesses (SMBs) in the U.S. play a role in our nation's cybersecurity? The U.S. Small Business Administration classifies 99.7% of American companies as small businesses. Small businesses pay 44% of the U.S. private payroll. They have generated 64% of net new jobs over the past 15 years, created more than half of the non-farm private GDP, and hired 40% of high tech workers (such as scientists, engineers, and computer programmers). Small businesses are a key segment to our nation's success. It is imperative that they protect their operations, staff and customers.



www.securingourecity.org

"The most common threat to your company is negligence, accounting for 39% of the breaches in the study. The average organizational cost of a data breach is \$5.5 million and the average cost per record is \$194."

—2011 U.S. Cost of a Data Breach

"Confronted with both malicious and non-malicious threats from inside and outside the organization, companies must proactively implement policies and technologies to mitigate the risk of costly breaches."

—Dr. Larry Ponemon, chairman and founder of Ponemon Institute



STOP | THINK | CONNECT™

© 2013 Securing Our eCity Foundation. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET. All other names and brands are registered trademarks of their respective companies.

201213-11-00V1

What are you
doing to protect
your business?

Into the Breach

A GUIDE TO CYBERCRIME TRIAGE



Top 10 ways to PREVENT AN ATTACK

- 1 CREATE AND IMPLEMENT A CYBERSECURITY POLICY AND PROCEDURES DOCUMENT**
- 2 EDUCATE ALL STAFF ON SAFE CYBERSECURITY PRACTICES:**
 - Use strong passwords; appropriately change and protect them
 - Identify and avoid spam and phishing
 - Recognize the latest social engineering tactics
 - Only disclose personal information on reputable sites and a secure network connection
 - Include a summary of the company's cyber security policies in a "Log-in" banner that users must acknowledge every time they log into the network
- 3 REGULARLY TRACK AND VERIFY YOUR COMPANY'S COMPLIANCE**
- 4 BE SUSPICIOUS OF ANY ANOMALOUS COMPUTER OR NETWORK BEHAVIOR**
- 5 IMPLEMENT NETWORK AND END-POINT SECURITY**
- 6 IDENTIFY WHERE AND WHAT INFORMATION RESIDES ON YOUR NETWORK CONNECTION**
- 7 RESTRICT ACCESS TO RESOURCES AND INFORMATION TO THOSE THAT ACTUALLY NEED IT**
- 8 DEVELOP STRONG BACKUP POLICIES AND PROCEDURES:**
 - Consistently backup data and test its reliability
 - Image or retain hard drives from employees who have departed and have had access to sensitive data
 - Take compromised servers offline or image and then restore them from backups
 - Enable computer and network logging and store logs offline
 - Treat every cyber incident as potentially malicious until it is determined otherwise

Top 3 Information SECURITY THREATS

- 1 DISGRUNTLED OR SOCIOPATHIC INSIDERS AND RECENTLY SEPARATED EMPLOYEES WITH TRUSTED ACCESS**
- 2 POOR INFORMATION SECURITY POLICIES AND PRACTICES INCLUDING:**
 - Poor password policies
 - No use of multi-factor authentication
 - Overuse of administrative authority
 - Failure to segment the network (*not everyone needs access to everything*)
 - Poor implementation of remote and/or wireless access
 - Poor backup policies and procedures
- 3 MISHANDLING OF PERSONALLY IDENTIFIABLE INFORMATION**

How can you help ensure your company is taking appropriate actions to protect your customers and your business? The easiest way to save your small business from loss of time and money due to cyber incidents is to prevent them from occurring in the first place. Preventive measures are only marginally expensive and invasive, but could ultimately save your company.

What are cybersecurity incidents? Any computer or network-related incident that disrupts normal business processes is considered a cybersecurity incident. Many malicious attacks stem from phishing attacks, spam and other unsolicited computer communication. These can lead to larger problems such as data breach, identity theft and Distributed Denial of Service (DDoS) attacks.

Will my business be 100% safe if I follow these guidelines? Good corporate cybersecurity practices go a long way to prevent breaches and keep your business, employees and customers safe. However, no system is completely invulnerable. You can make a difference in the preservation of important data by anticipating or recognizing an attack and responding to it quickly and effectively. When your system is breached every second is crucial.

Top 5 Steps to RESPOND TO ATTACKS

- 1 CONTACT AUTHORITIES** (*See back panel*)

Fast responses are important in cases with active data exfiltration such as customer or financial data.
- 2 PRESERVE THE ORIGINAL HARD DRIVES OF COMPROMISED SYSTEMS**

Provide documentation for anything that has been done to the system since the discovery of the incident.
- 3 PROVIDE COPIES OF ANY NETWORK DIAGRAMS OR SYSTEM DOCUMENTATION SHOWING THE ENVIRONMENT IN WHICH THE SYSTEM OPERATED**
- 4 IDENTIFY AND COPY ANY INTERNAL OR EXTERNAL LOG FILES, INCLUDING INTRUSION DETECTION SYSTEM AND FIREWALL LOGS**
- 5 CONSIDER MONITORING THE SYSTEM'S NETWORK CONNECTIONS PRIOR TO TAKING IT OFFLINE**

Other compromised systems or suspect IP addresses can frequently be identified.

What is some of the key information you should record for reference?

- IP address of compromised system
- Hostname or NetBios Name
- Operating System and version
- Use of DHCP or static IP address assignment
- Date and time of incident and response
- Network Topology
- Applications and processes running
- Impact (cost to restore/examine/investigate)
- Policies and procedures