THE CYBER THREAT TO SMALL AND MEDIUM SIZED BUSINESSES IS REAL

Unauthorized Access

"One of our up-and-coming salespeople left for a competitor…Several months later, the management team noticed a disturbing trend: The company kept losing bids for new business to this same competitor. When it had happened four times in a row, we realized that we'd forgotten to turn off the former employee's network access. He had been logging into our network, stealing our information, and undercutting us" – SMB Owner [6]

"Small businesses continue to be the most victimized of all companies" [1]

Data Loss

"A New York mannequin maker learned the hard way, in 2012, when he lost $1.2 million within a matter of hours through a series of fraudulent wire transfers. Cybercriminals breached his 100-employee firm and got its online banking credentials. The company's anti-virus (AV) software never detected anything." [5]

Hacking

"When the FBI contacted us, we thought it was a prank. They said our website had been compromised and they wanted access to our site to observe where the traffic was coming from. The FBI then advised us to rebuild the site from scratch, which cost a few thousand dollars… Some internet providers are still blocking the URL for security reasons. We could be losing business if potential clients are trying to reach the website but can't" – SMB Owners [1]

Malware

"Cyber thieves planted a (hidden) software program on the cash registers at two Chicago-area magazine shops that sent customer credit-card numbers to Russia. The credit card company demanded an investigation, at the owner's expense, and the whole ordeal left him out about $22,000." [2]

"Cyber criminals are targeting SMBs because they have limited time and resources for security yet have a lot of the same valuable information that larger business have." [4]

"552 Million – Identities exposed in 2013 up 493% from 93 million in 2012." [3]

"Cyberattacks on small businesses with fewer than 250 employees represented 31% of all attacks in 2012, up from 18% in the prior year." [3]

243 – Median number of days attackers were present on a network before detection

"Small businesses can't afford to remain complacent or ignorant about the risk of being a cyberattack target." [1]

The IC Analyst – Private Sector Program
Mission Statement

"This program enables intelligence community analysts and private sector partners to gain a greater understanding of how their disparate, yet complementary, roles can work in tandem to ensure mission success."

"Cyber criminals are targeting SMBs because they have limited time and resources for security; yet, they have a lot of the same valuable information as larger business." [4]

"552 million identities exposed in 2013. This is up 493% from 93 million in 2012" [3]

"Small businesses can't afford to remain complacent or ignorant about the risk of being a cyber-attack target." [1]

Bulk Data Intrusion Working Group Contributors

References:

1. CNN
2. Wall Street Journal
3. Symantec
4. Ross
5. FireEye
6. Forbes
7. National Cyber Security Alliance

Understanding Cyber Threats

A Guide for Small and Medium Sized Businesses

Publication of the 2014 Office of the Director of National Intelligence
Intelligence Community Analyst – Private Sector Program

THE FUNDAMENTALS OF CYBER SECURITY

"Eighty percent of the intrusions of your networks today can be handled by patches, anti-virus and user actions. We spend 90 percent of our time on the 80 percent of the issues that could be handled by good hygiene."
- Brigadier General Paul Nakasone
Deputy Commander,
U.S. Army Cyber Command

Key Terms

Antivirus (AV) – *Antivirus is software used to detect malicious code.*

Firewall – *A firewall is a security device that enforces network access through a defined policy which authorizes or rejects network traffic between a trusted and untrusted zone.*

Phishing – *Phishing is a targeted e-mail spoofing campaign directed at a specific population or company. Phishing seeks unauthorized access to confidential data by masquerading as a trusted entity. Phishing differs from spear phishing because it is more general in nature and is directed at a larger population.*

Spear Phishing – *Spear phishing is a targeted e-mail spoofing campaign directed at a limited number of individuals. Spear phishing seeks unauthorized access to confidential data. These campaigns often leverage malware and are extremely difficult to detect.*

Intrusion Detection System (IDS) – *This tool is a passive tool that monitors network traffic and alerts the administrator of potential threats. An IDS is generally used for monitoring only; unlike the IPS it will not take actions to actively stop an attack.*

Intrusion Prevention System (IPS) – *This tool prevents intrusions by monitoring network traffic for malicious activity and blocking malicious traffic, dropping packets identified as malicious, blocking traffic from source IP addresses, and notifying the administrator of threats.*

CYBER SECURITY

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

IMPLEMENTATION

Cyber security is not just your antivirus and firewalls, it encompasses technology, physical security, policy, employee education, threat intelligence and more.

CYBER THREATS

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

WHO IS IMPACTED

Cyber threats impact all industries at all levels. No industry or business size is immune from cyber attack. Recognizing you are a target is the first step to protecting your business.

"91% - Increase in spear phishing email campaigns in 2013" [3]

"60% - Small businesses will close within six months of a cyber attack." [7]

WHAT IS YOUR COMPANY CYBER SECURITY STRATEGY?

UNDERSTAND YOUR RISK

What are my risks and how do I determine them?

What do I need to protect and how do I protect it?

How good is my cyber hygiene?

INTERNAL CYBER LANDSCAPE

How much money, resources, and people do I have for cyber security?

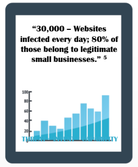
Do I share any sensitive data with partners/vendors and how secure are they?

What is my core business strategy and how does security fit in?

PROTECTING ASSETS

Should I outsource or keep IT in house?

Are my online practices putting my business or customers at risk?



HOW DO I IDENTIFY AND DETECT CYBER PROBLEMS?

There are many signs that may seem innocuous but may actually be the result of a larger problem or cyber-attack. This can be your workstation running exceptionally slow, a program behaving abnormally, pop-ups ads, unexpected password prompts, misspelled website names, unexpected emails or attachments, etc.

"30,000 – Websites infected every day; 80% of those belong to legitimate small businesses." [5]

Additional Resources

- **sectools.org** – Cyber Security Tools
- **ic3.gov** – Internet Crime Complaint Center
- **staysafeonline.org** – National Cybersecurity Alliance
- **us-cert.gov/ncas/tips** – General Resources, Tips, News
- **dhs.gov** – Stop Think Connect DHS Cyber Security Campaign
- **us-cert.gov/home-and-business** – Resources for Home and Business
- **sba.gov** – Resources for Home and Business

HOW TO PROTECT YOUR COMPANY

Know what data you have and what you need to do to protect it. This can be credit card information, email addresses, Intellectual property, trade secrets, user names, Personally Identifiable Information, HIPAA, customer information etc. Even the smallest piece of information can provide hackers with a foot in the door.

THIS IS THE MOST IMPORTANT STEP

Step 1 – Develop a Cyber Security Strategy

Step 2 – Educate Employees

Educating employees on cyber security is one of the most effective ways to keep your business secure. The more an employee knows about how to identify and avoid threats the safer your business will be. Educating employees does not have to be expensive as there are countless free resources online.

Step 3 – Implement Technologies

Employing technologies for your business does not necessarily have to be expensive. There are several cost effective, free, and open source technologies that you can use to keep your business safe. This includes Antivirus, IDS, IPS, and firewalls. It's important to protect all of your devices that connect to the Internet including computers, smart phones, gaming systems, etc. Any device can be a vector of attack.

Step 4 – Practice the Essentials

What are the essential things I should do to be safe?

Technology to Use
Make sure your AV is running and up to date. Enable auto update and regular scanning.
Use security applications on your smart phone
Run a firewall and anti-malware program. These may already be bundled in your Antivirus.

Securing Software
Make sure all your software and applications are up to date on any device that connects to the internet. Any outdated and unpatched program or device can be a vector of attack for a cyber-criminal.

Protecting Your Sensitive Data
Password protect and/or encrypt your sensitive files and information especially before sending it to others. Consider using an encrypted VPN connection to the internet.

Maintain Good Cyber Hygiene
Passwords/Logins
Make sure your passwords are strong and only used once per system/site
Frequently change your passwords
Never share your password
Change all default passwords for anything that connects to the internet, especially routers. Attackers can easily find default passwords and access your devices.

Limit Personal Information Posted Online
Limit the amount of information you post about yourself and your business online especially on social media. Attackers can use this information to spoof your identity, send out fake emails, or use it as part of their cyber-attack puzzle.

UNDERSTAND THIRD PARTY RISKS

Make sure your connections with business partners are secure. Ensure that you are aware of who is allowed to view what data and what their cyber practices are. Any connection can be a vector of attack into your or other network.

HOW DO I RECOVER FROM AN INCIDENT?

Backup and recovery plans should be made beforehand so you know how to deal with an incident when it arises. You should identify the point at which you may need to call someone in and who that person should be. When necessary you may have to report a breach to law enforcement agencies as well as your customers.