SBIR · STTR
America's Seed Fund™
POWERED BY SBA

COURSE 10, TUTORIAL 1

THE IMPACT OF CYBERSECURITY ON SMALL BUSINESS

Cybercrime is growing as use of the Internet and business networks expand. Today, more than ever, businesses of all sizes rely on their networks, data and internet connectivity to conduct business. According to a McKinsey Global Institute report the Internet's economic impact has been greatest among "individual consumers and small, upstart entrepreneurs." The Internet allows even the smallest firms to have a global impact. What began as an obscure network for researchers and scientists a few decades ago has grown into an $8 trillion a year e-commerce enterprise connecting over two billion people.[1]

As the use of Internet and networked computers grows, and new technologies such as cloud computing enable even greater technological advances, the occurrence of cybercrime is expected to grow as cybercriminals seek to exploit online and networked vulnerabilities in business networks. Cybercrime costs the global economy about $445 billion every year, with the damage to business from theft of intellectual property exceeding the $160 billion loss to individuals.

A GROWING CONCERN FOR SMALL BUSINESS

Cybercrime is becoming a growing and significant concern for small business. In its 2014 Year-End Economic Report, the National Small Business Association, also known as NSBA, found that "half of all small businesses report they have been the victim of a cyber attack – up from 44 percent just two years ago."[2] "Among those who were targeted, 68 percent reported being a cyber-victim more than just once."[3]

"Fifty percent of small to medium-sized businesses (SMB) have been the victims of cyber attack and over 60% of those attacked go out of business."

Dr. Jane LeClair
Chief Operating Officer
National Cybersecurity Institute

Despite the rise in cybercrime among small businesses, many small businesses remain susceptible to cyber attacks due to lack of resources and surprisingly, a lack of knowledge of the threat. The NSBA found that despite the increasing threats posed by cyberattacks, an astounding one in four small business owners have "little to no understanding of the issue whatsoever." Dr. Jane LeClair, the Chief Operating Officer of the National Cybersecurity Institute, noted in testimony to the House Committee on Small Business that small to medium-sized businesses, also known as SMBs "are challenged both by the ability and the desire to secure themselves against cyberthreats which makes them uniquely vulnerable to cyber attacks. Fifty percent of SMB's have been the victims of cyber attack and over 60 percent of those attacked go out of business. Often SMB's do not even know they have been attacked until it is too late."[5]

More than ever, sensitive data, intellectual property and personal information of small and medium sized firms are targeted by an ever increasing and sophisticated community of cybercriminals. Symantec found that in the last five years, a steady increase in cyber attacks targeting businesses with less than 250 employees had been observed, "with 43 percent of all attacks targeted at small businesses in 2015, proving that companies of all sizes are at risk."[6]

Small business is an increasingly attractive target for cybercrime. By themselves, individual small businesses may not appear to present an overly attractive target. However, collectively small businesses are a very lucrative target set due to the collective economic impact of small business. According to the Small Business Administration (SBA), small businesses make up 99.7 percent of U.S. employer firms; 63 percent of net new private-sector jobs; 48.5 percent of private-sector employment; 42 percent of private-sector payroll; and 46 percent of private-sector output.[7]

In addition, small business attacks are increasing because they present cybercriminals with an easy way to gain access to customer credit card records and bank accounts, supplier networks and employee financial and personal data. Smaller companies tend to have weaker online security. They're also doing more business than ever online via cloud services that perhaps don't use strong encryption technology. "SMB's have resource constraints and often ignore cybersecurity in favor of day-to-day operations or other financial needs. Yet SMB's remain a gateway to gain access to clients, business partners, donors, and contractors working with the SMB … a backdoor into many large organizations."[8] "To a hacker, that translates into reams of sensitive data behind a door with an easy lock to pick."[9] If a small business has any Fortune 500 companies as customers, they are an even more "enticing target" — they are an "entry point."[10] This is an increasingly common type of cyberattack known as a secondary attack.

Interesting statistics from the SBA

Small businesses make up

- **99.7%** of U.S. employer firms
- **63%** of net new private-sector jobs;
- **48.5%** of private-sector employment;
- **42%** of private-sector payroll; and
- **46%** of private-sector output.

SUSCEPTIBILITY TO EMAIL ATTACKS

Small businesses are particularly vulnerable to email attacks "closely mimicking those of banks or other trusted institutions and citing an urgent need to login to an account or provide some other vital information" since multiple employees could have access to vital information. "Further, business accounts do not enjoy the same level of protections and guarantees against loss and theft as those provided to consumers—a reality that many small business owners do not discover until it is too late. Consumers are protected by Regulation E, which dramatically limits their liability in a cyber-heist. Commercial accounts, however, are covered by the Uniform Commercial Code (UCC). The UCC does not hold banks liable for unauthorized payments so long as 'the security procedure is a commercially reasonable method of providing security …' Few small businesses that are the victims of theft from their bank accounts ever recover those funds."[11]

The cost of cybercrime to a small business can be devastating. In 2013, cyberattacks cost small businesses on average, $8,699 per attack. Today, that number has skyrocketed to $20,752 per attack. "For those firms whose business banking accounts were hacked, the average losses were $19,948 today – up significantly from $6,927 in 2013. This huge jump in cost is likely due to the increased sophistication in phishing and hacking schemes as well as an improved economy that finds greater funds available in many small firms' bank accounts than was there just two years ago."

It is clear that small businesses need to be better informed on the impact cyberattacks can have on their businesses and be better prepared to meet the increasing cyberthreat.

ENDNOTES

1. "The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity," McKinsey Global Institute, October 2011, http://www.mckinsey.com/~/media/McKinsey/Industries/High%20Tech/Our%20Insights/The%20great%20transformer/MGI_Impact_of_Internet_on_economic_growth.ashx

2. "2014 Year-End Economic Report," National Small Business Association (NSBA), 2014 ["Methodology: The 2014 Year-End Economic Report was conducted on-line Dec. 29, 2014 – Jan. 12, 2015 among 675 small-business owners— both members and nonmembers of NSBA— representing every industry in every state in the nation."], http://www.nsba.biz/wp-content/uploads/2015/02/Year-End-Economic-Report-2014.pdf

3. "2014 Year-End Economic Report," National Small Business Association (NSBA), 2014 ["Methodology: The 2014 Year-End Economic Report was conducted on-line Dec. 29, 2014 – Jan. 12, 2015 among 675 small-business owners— both members and nonmembers of NSBA— representing every industry in every state in the nation."], http://www.nsba.biz/wp-content/uploads/2015/02/Year-End-Economic-Report-2014.pdf

4. "2013 Small Business Technology Survey," National Small Business Association (NSBA), 2013, http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf

5. "Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks," Statement for the Record: Dr. Jane LeClair, Chief Operating Officer, National Cybersecurity Institute at Excelsior College Before the United States House of Representatives Committee on Small Business, 4/22/15, http://smbiz.house.gov/UploadedFiles/4-22-2015__Dr.__LeClair__testimony.pdf

6. "ISTR: Internet Security Threat Report," Symantec, volume 21, April 2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_14823723&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2

7. "Frequently Asked Questions – Advocacy: The Voice of Small Business in Government," SBA (Small Business Administration) Office of Advocacy, March 2014, http://www.sba.gov/sites/default/files/FAQ_March_2014_0.pdf

8. "Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks," Statement for the Record: Dr. Jane LeClair, Chief Operating Officer, National Cybersecurity Institute at Excelsior College Before the United States House of Representatives Committee on Small Business, 4/22/15, http://smbiz.house.gov/UploadedFiles/4-22-2015__Dr.__LeClair__testimony.pdf

9. "Why Your Business Might be a Perfect Target for Hackers," Inc. Magazine, December 2013/January 2014, http://www.inc.com/magazine/201312/john-brandon/hackers-target-small-business.html

10. "Why Your Business Might be a Perfect Target for Hackers," Inc. Magazine, December 2013/January 2014, http://www.inc.com/magazine/201312/john-brandon/hackers-target-small-business.html

11. "Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks," Testimony of Todd McCracken, President and CEO, NSBA (National Small Business Association), House Committee on Small Business Hearing, 4/22/15, http://smbiz.house.gov/UploadedFiles/4-22-2015_McCracken_Testimony.pdf

12. "2014 Year-End Economic Report," National Small Business Association (NSBA), 2014. ["Methodology: The 2014 Year-End Economic Report was conducted on-line Dec. 29, 2014 – Jan. 12, 2015 among 675 small-business owners— both members and nonmembers of NSBA— representing every industry in every state in the nation."], http://www.nsba.biz/wp-content/uploads/2015/02/Year-End-Economic-Report-2014.pdf