Cybersecurity Workbook

AMERICA'S SBDC IOWA

cybersecurity

definition: measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

COMMON THOUGHTS AND PERCEPTIONS

- Why worry about cybersecurity?
- Only big companies need to worry about cybersecurity.
- My business is too small. We don't have anything worry about.
- My business doesn't collect any valuable information.
- I'm not worried, cyberattacks won't happen to us.
- Cybersecurity was first used in 1989.

What is cybersecurity? According to the Merriam-Webster dictionary, cybersecurity is defined as measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack. The threats and aftermath of cybersecurity breaches are all around us. Media report regularly on the latest data breach and the hundreds, even thousands of records that were compromised.

But why should a small business worry about cybersecurity? Most of the headlines surrounding cyberattacks involve large corporations. They do not report on the attacks against small businesses. The truth is, cyberattacks against small businesses do happen. According to a report by Verizon, 71% of data

breaches they investigated were targeted at small businesses with less than 100 employees. Of this group, businesses that had less than 10 employees were the most frequently targeted and attacked.

Small Business Cybersecurity Statistics

- 43% of cyberattacks target small business
- 60% of small businesses go out of business within 6 months of a cyberattack
- 48% of data breaches are caused by acts of malicious intent. Human error or system failure account for the rest

2

Small Business Cybersecurity Attack Statistics

A recent study by Ponemen Institute surveyed small business with a range of less than 100 employees to 1,000 employees. The survey asked small businesses if they had experienced a cyberattack or data breach during the time period of May 2015 to May 2016.

- 55% of respondents said their companies had experienced a cyberattack during the 12 month period
- 50% of respondents said they had experienced a data breach that involved customer and employee information during the time period

The businesses affected by the cyberattacks reported that on average they spent $879,582 because of damage or theft of IT assets. Additionally, the disruption to the normal operations of their business cost on average $955,429. Not only do businesses have to pay for the actual damages caused, they are also losing revenue. It's no wonder why 60% of small businesses go out of business within 6 months of a cyberattack. The amount of money needed to recover can be insurmountable to some businesses. This does not even consider the loss of trust from their customers due to the event.

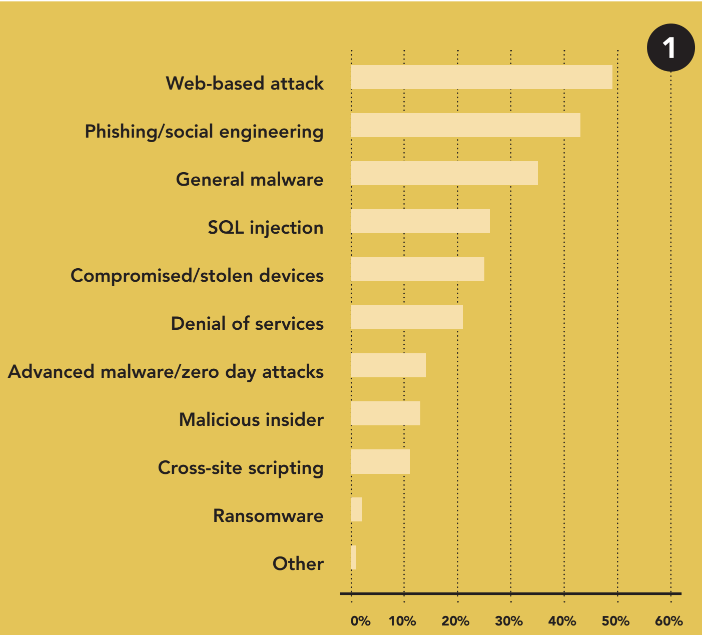
So how are small businesses being attacked? What type of attacks have small businesses experienced?

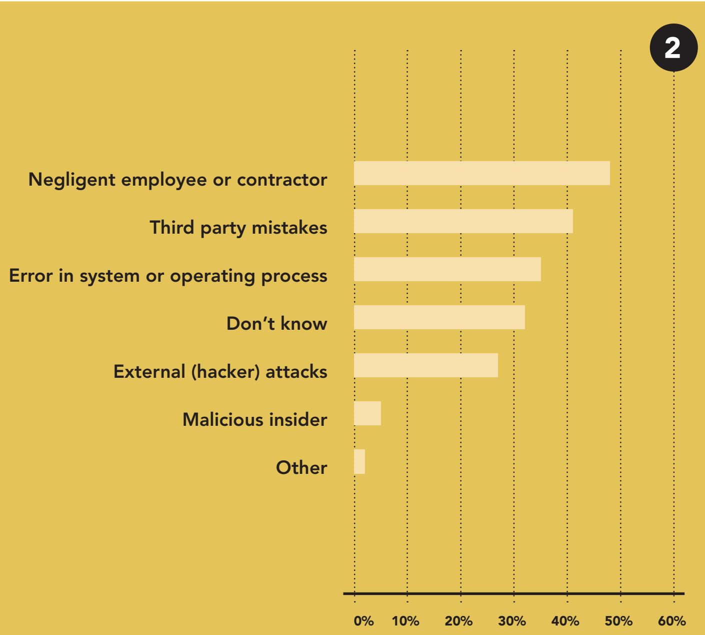
1. See chart at right. ▶

How is data being compromised in small businesses? What is the cause of the data breach?

Turns out that 48% of respondents said the data breach was due to a negligent employee or contractor and 41% reported third-party mistakes were the cause. The survey also indicated that 32% of small businesses could not identify the cause of the data breach.

2. See chart at far right. ▶

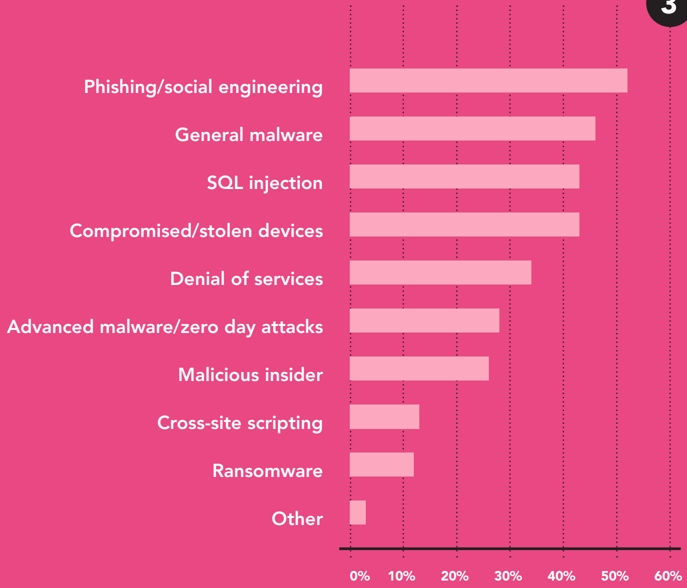

1
Web-based attack
Phishing/social engineering
General malware
SQL injection
Compromised/stolen devices
Denial of services
Advanced malware/zero day attacks
Malicious insider
Cross-site scripting
Ransomware
Other
0%
10%
20%
30%
40%
50%
60%


2
Negligent employee or contractor
Third party mistakes
Error in system or operating process
Don’t know
External (hacker) attacks
Malicious insider
Other
0%
10%
20%
30%
40%
50%
60%

3

4

3


Phishing/social engineering
General malware
SQL injection
Compromised/stolen devices
Denial of services
Advanced malware/zero day attacks
Malicious insider
Cross-site scripting
Ransomware
Other
0%
10%
20%
30%
40%
50%
60%

Where are the most vulnerable points of entry for a cyberattack? How are hackers getting into small business networks?

◀ ***3. See chart at left.***

The National Institute of Standards and Technology (NIST) has developed a framework to help businesses think through, assess, evaluate, and develop a plan to help reduce the risk of becoming a victim of a cyberattack.

The NIST Framework has five parts. Below is a summary of these parts and what they mean to a business.

- ⦿ **Identify** – Organizational understanding to manage cybersecurity risks to systems, assets, data, and capabilities
- ⦿ **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical infrastructure service
- ⦿ **Detect** – Develop and implement appropriate activities to identify occurrence of cybersecurity event
- ⦿ **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity event
- ⦿ **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

Ten Cybersecurity Tips for Small Businesses

1. Protect information, systems, & networks from damage by viruses, spyware, & other malicious code

2. Provide security for Internet connection

3. Install & activate software firewalls

4. Patch all operating systems & applications

5. Make backup copies of important business data & information

6. Control physical access to business computers & network components

7. Secure wireless access points & networks

8. Train employees in basic security principles

9. Require individual accounts for each employee using business computers & business applications

10. Limit access to data & information by employees, & limit the authority to install software

What does Iowa law say about data breaches? What requirements do you need to address if you have a data breach? Who do you need to notify? What does a data breach mean? What type of information do you need to worry about being accessed?

Iowa law (Iowa Code Chapter 715C) defines a security breach as any unauthorized acquisition of personal information "maintained by a person in any medium, including on paper, that was transferred by the person to the medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information."

What is meant by personal information? Personal information can include

- Social Security number
- Driver's license or government identification number
- Financial account numbers
- Credit or debit card numbers along with expiration date or other security that would permit access to a financial account
- Unique biometric data

When do you need to report a security or data breach? According to Iowa law you must provide written notice to the Attorney General's Consumer Protection Division Director when a security breach affects at least 500 residents in Iowa and within 5 days of notifying the affected individuals. To report a security breach, go to the Attorney's General website – www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/

What can a small business do to help protect their business and safeguard their information? Businesses need to assess their risk and evaluate what they should be aware of to reduce the risk.

Checklist for Small Businesses

There are practices and measures that every business can implement to help. The information here is a start and discusses basic security practices. Some businesses may have more complex needs and should consult experts for additional assistance. This is not a comprehensive list of all possible security practices and ideas. Some practices may depend on the industry and compliance with any regulations.

Technology Inventory

What kinds of technology do you utilize in your business?

- ⊙ Computer
- ⊙ Laptop
- ⊙ Email
- ⊙ Wi-Fi
- ⊙ Router
- ⊙ Firewall
- ⊙ Virtual Private Networks (VPN)
- ⊙ Social Media/ Networking
- ⊙ Website
- ⊙ Mobile devices
- ⊙ Copiers/Printers/ Fax Machines
- ⊙ Cloud solutions
- ⊙ USB
- ⊙ Internet of Things (IoT) – other devices connected to the Internet

Each of these items comes with a security risk due to the fact they are connected to the Internet and interact with other devices. Assessing the risk of each technology item in your business will allow you to identify best practices to reduce the risk of a security breach.

Passwords

Passwords are the most common defense against unauthorized access to computers and systems. What can be done to make passwords as effective as possible?

Do

- ✓ Include a mix of upper and lowercase letters, numbers, and special characters
- ✓ Use a long phrase such as SmallbusinessesInIowaRock123
- ✓ Use a different password for each different account
- ✓ Utilize a password manager for tracking multiple passwords
- ✓ Utilize 2 Factor Authentication when possible. Factor 1 is something that you know such as your password and Factor 2

is something that you have such as a text message sent to your phone

✓ Change your password on a regular basis

Don't

✓ Use personal information as part of your password

✓ Store your passwords on a piece of paper near your computer

✓ Use the same password for multiple accounts

✓ Share your password with anyone

Identify Important Information

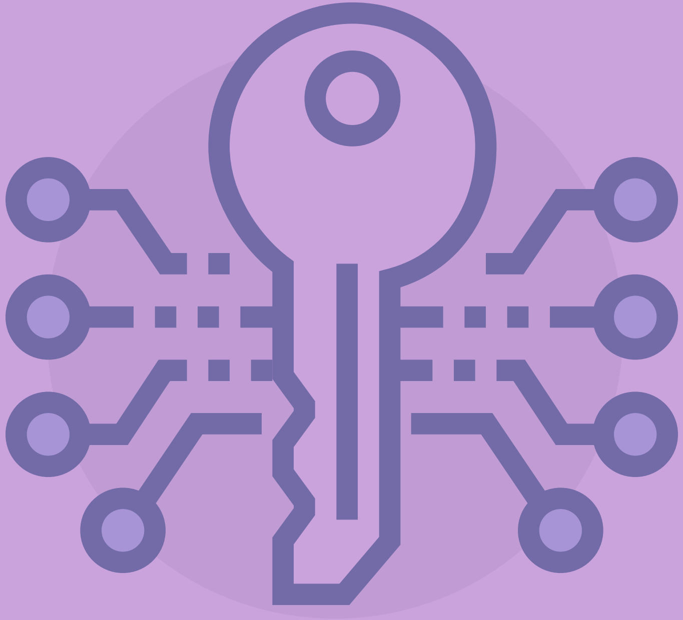
What types of client and employee data do you store electronically? Which pieces of information would be valuable if they fell into the wrong hands? Which of these types of information do you store and how are they stored?

- ⦿ Full name
- ⦿ Home address
- ⦿ Email address
- ⦿ National identification number
- ⦿ Passport number
- ⦿ IP address when linked to other items
- ⦿ Vehicle registration plate number
- ⦿ Driver's license number
- ⦿ Face, fingerprints, or handwriting
- ⦿ Credit card information
- ⦿ Digital identity
- ⦿ Date of Birth
- ⦿ Birthplace
- ⦿ Telephone number
- ⦿ Login names
- ⦿ Mother's maiden name

Are you collecting any of the above types of information that you really don't need? Are there any of these that you do not need to collect anymore?

Personal information that is stored on any electronic components or devices in your business should be encrypted and not transmitted carelessly.

Stay secure…



Data Backups

Where do you store your data? Do you have a copy of your important business information? Where is the copy stored? Do you store information in the cloud? On an external hard drive? Separate server?

Regular backups of your data is important. Equipment can fail, be stolen, or even lost. Regularly scheduled backups are important to ensure the security of your information. Make sure the backup is stored somewhere offsite. Cloud based storage of information is a secure way to store data.

Wireless Internet

Connecting to public wireless networks can leave you open to a cyberattack. Public wireless networks allow anyone to connect and make it easy for hackers to intercept any information that you transmit over the wireless network. If you need to connect to an unknown wireless network, make sure it is a legitimate wireless network and check that your Internet traffic is encrypted by examining the security certificate of all websites to make sure your traffic has not been manipulated.

When you are setting up your own wireless network make sure to change the network name to something that is unique and does not give away any personal information. Also, be sure to enable wireless encryption and utilize a long, complex password. Be sure to change the administrator password frequently and when individuals with the information leave the company. Make sure to check with the manufacturer of your device for any updates on a regular basis.

Make sure public wireless networks include **encryption**

Security Training and Awareness

Employees are truly the first line of defense when it comes to protecting client information. Make sure your employees understand the importance of protecting sensitive information. As a best practice you should train your employees on the items below.

- Overall security policy of the business
- Proper use of computers, networks, & Internet connections
- Any limitations on the personal use of phones, computers, printers, or any other business resource
- Any restrictions on working from home and/or processing business data offsite

Once employees are trained and understand the security measures of the business, request them to sign a statement saying they understand and will follow the business policies. Also, make sure they understand the consequences and penalties for not following the policies.

After assessing your risk of a cyberattack and learning basic security best practices, it is time to develop a plan of what to do if a data breach does happen. It is better to think through the steps before it happens and to be proactive.

Before a security breach occurs, be prepared by going through and knowing the answers to the following questions.

Employees are the **first** line of defense

KNOW YOUR DATA

Where is your data stored?

How does it flow in your business?

Who has access to your data?

Is the data encrypted?

Is the data considered to be sensitive or only parts of it?

HOW IS THE DATA MONITORED

Is there log or place that records touches with the data?

Know who **sees** your data

Where is the backup of data located?

UNDERSTAND YOUR DATA

Why is it valuable?

Who would want to steal the data?

PEOPLE TO INVOLVE

➡ **Know who to call for help**

Internet Service Provider

Attorney

Insurance Agent

Accountant

Identify those who
can help when needed

Any additional software as a service providers

Advisors

Other

➡ **Identify which employees to involve**

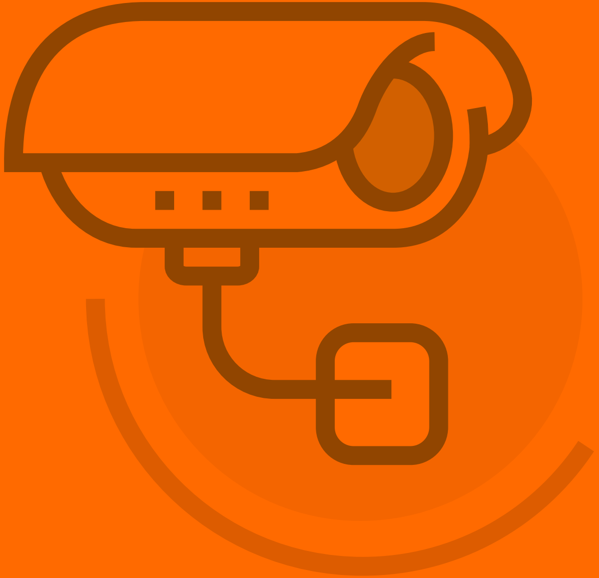
Business Owner

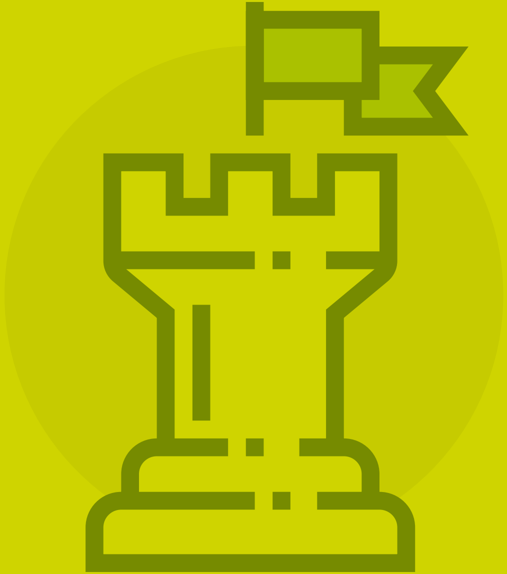
Manager

IT Staff

Know **who** has access to your system

…be watchful…





...play defensive

- **Know which outside experts to call**

IT Professional

Cybersecurity Expert

Other

POWERED BY
SBA
U.S. Small Business Administration

Funded in part through a Cooperative Agreement with the U.S. Small Business Administration. • Iowa State University does not discriminate on the basis of race, color, age, ethnicity, religion, national origin, pregnancy, sexual orientation, gender identity, genetic information, sex, marital status, disability, or status as a U.S. veteran. Inquiries regarding non-discrimination policies may be directed to the Office of Equal Opportunity, 3410 Beardshear Hall, 515 Morrill Road, Ames, Iowa 50011, Tel. 515-294-7612, emaileooffice@iastate.edu.

PROCESS TO FOLLOW

- Know what data you need to protect and where it is located
- Know which employees have access to key applications
- Understand the reporting requirements of a data breach
- Do a trial run of a data breach with your key employees

Additional Resources

America's SBDC Iowa – www.iowasbdc.org
National Institute of Standards and Technology (NIST) – www.nist.gov
Federal Trade Commission – Data Security – www.ftc.gov/datasecurity
Federal Bureau of Investigations (FBI) – www.fbi.gov/investigate/cyber
National Cyber Security Alliance – www.staysafeonline.org
Homeland Security – Stop. Think. Connect – www.dhs.gov/stopthinkconnect
Small Business Administration (SBA) – www.sba.gov/content/introduction-cybersecurity

*For a free assessment of your business with regards to cybersecurity and your risk, please visit America's SBDC Iowa website at **www.iowasbdc.org**. Here you will also find additional tools to help you and your business understand and protect against a cyberattack.*

AMERICA'S SBDC® IOWA

AMES, IOWA • 515-294-2030 • WWW.IOWASBDC.ORG