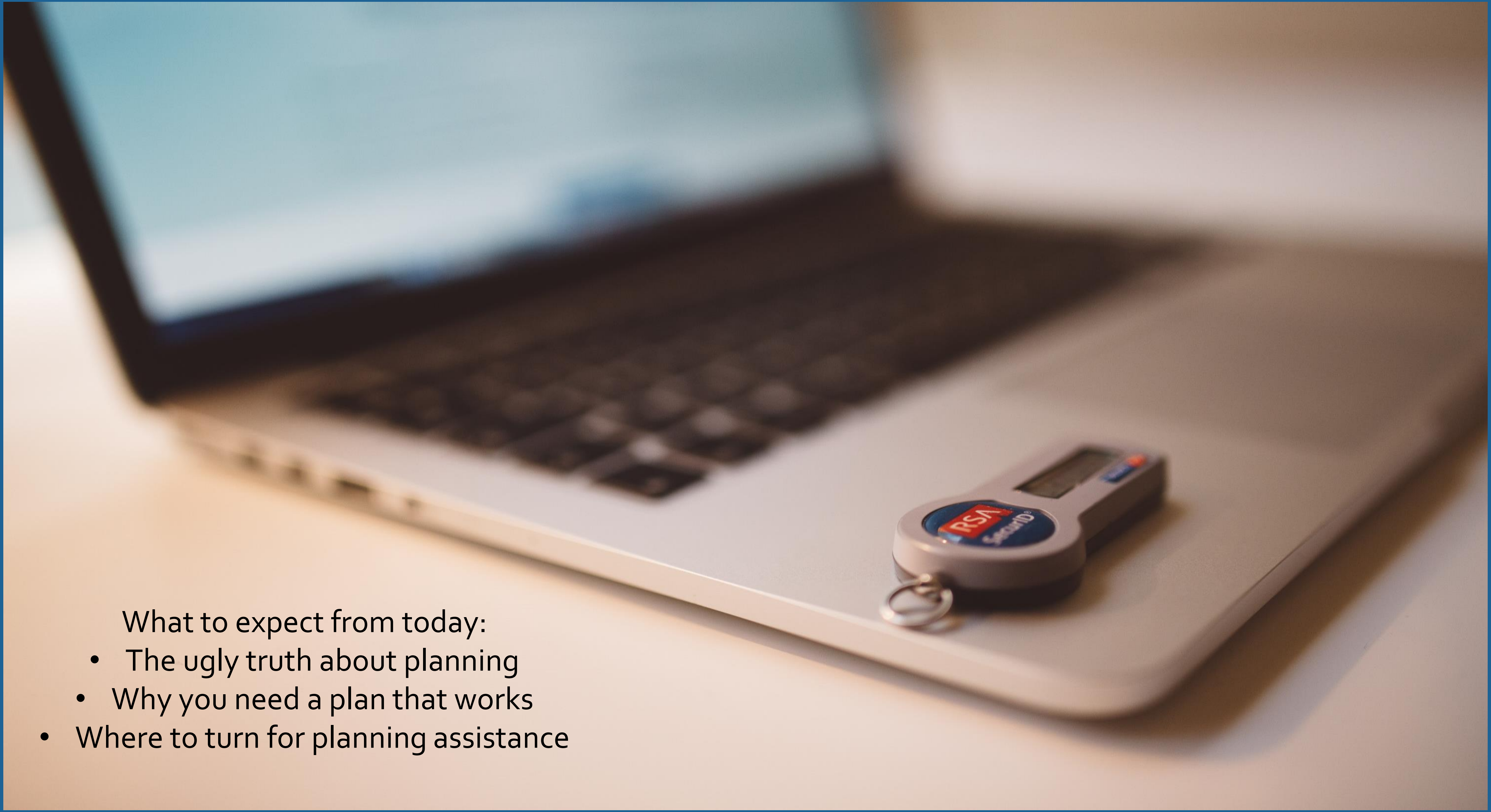
AMERICA'S SBDC KANSAS CYBER

Brian S. Dennis
Director
Cyber Security Center for Small Business
Kansas Small Business Development Center

AMERICA'S SBDC KANSAS

KU THE UNIVERSITY OF KANSAS

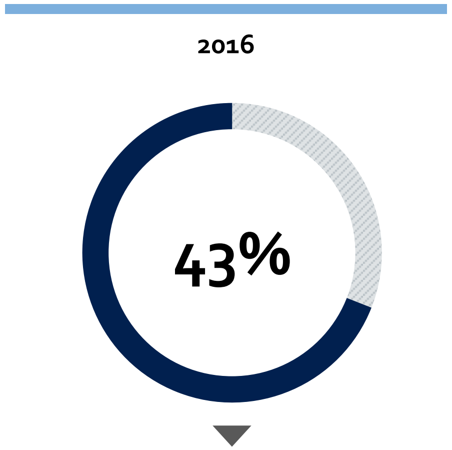


What to expect from today:

- The ugly truth about planning
- Why you need a plan that works
- Where to turn for planning assistance

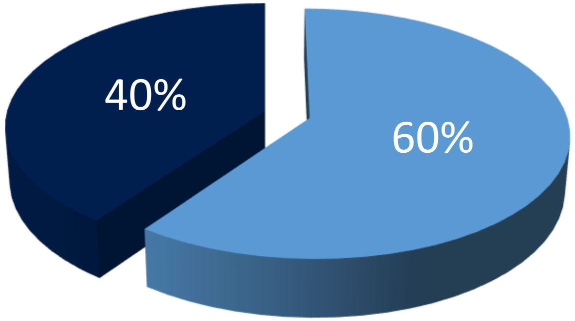
Small Businesses are a Target

According to Symantec, **Nearly HALF of all cyber-attacks are now levied against small businesses**



An attack can set a small business back anywhere from $54,000 to over $100,000 per incident (CNBC).

60% of companies breached never recover....



PCWorld in August 2013 reported that of the small businesses who suffered a breach, roughly 60 percent go out of business within six months after the attack.

Small Business Challenges

Staying ahead of the threat curve

- Lack of awareness of the threat
- Increased scrutiny and liability from buyers, business partners, etc.
- Business-wide education (not just technical—also behavioral)
- Cost of implementation of adequate protection
- Recovery after becoming victim
- Lack of support network

There is NO perfect plan!

- Raise awareness of cyber risk within Kansas’ small business community.

- Help businesses manage the threat and impact of cyber interference.

- Foster innovation in cyber security

DATA ASSURED™

Cyber Program Elements

Industry-Specific Training

ASBDC-KS Advisor Development

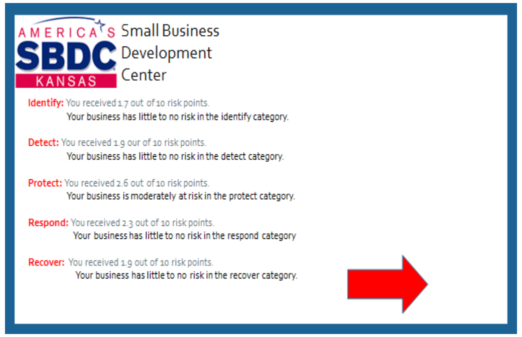
AMERICA'S SBDC KANSAS

Fostering Innovation

SBIR · STTR
America's Seed Fund

Custom Small Business Resources

Self Assessments



AMERICA'S SBDC KANSAS Small Business Development Center

Identify: You received 1.7 out of 10 risk points.
Your business has little to no risk in the identify category.

Detect: You received 1.9 our of 10 risk points.
Your business has little to no risk in the detect category.

Protect: You received 2.6 out of 10 risk points.
Your business is moderately at risk in the protect category.

Respond: You received 2.3 out of 10 risk points.
Your business has little to no risk in the respond category

Recover: You received 1.9 out of 10 risk points.
Your business has little to no risk in the recover category.

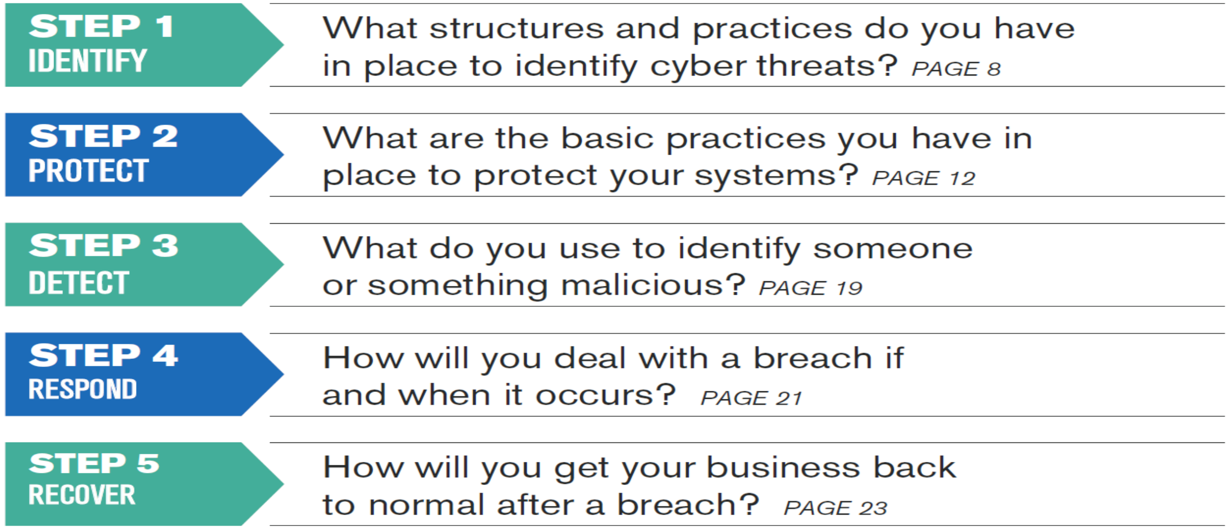
Business Continuity Planning

- Launching in Fall of 2017 to assist Kansas’ small business community to make a reasonable effort to protect their critical data and infrastructure

- Based off the NIST Framework

- Serves as the foundation for KSBDC trainings and counseling efforts

- Designed as a functional tool, not white paper or scare tactic

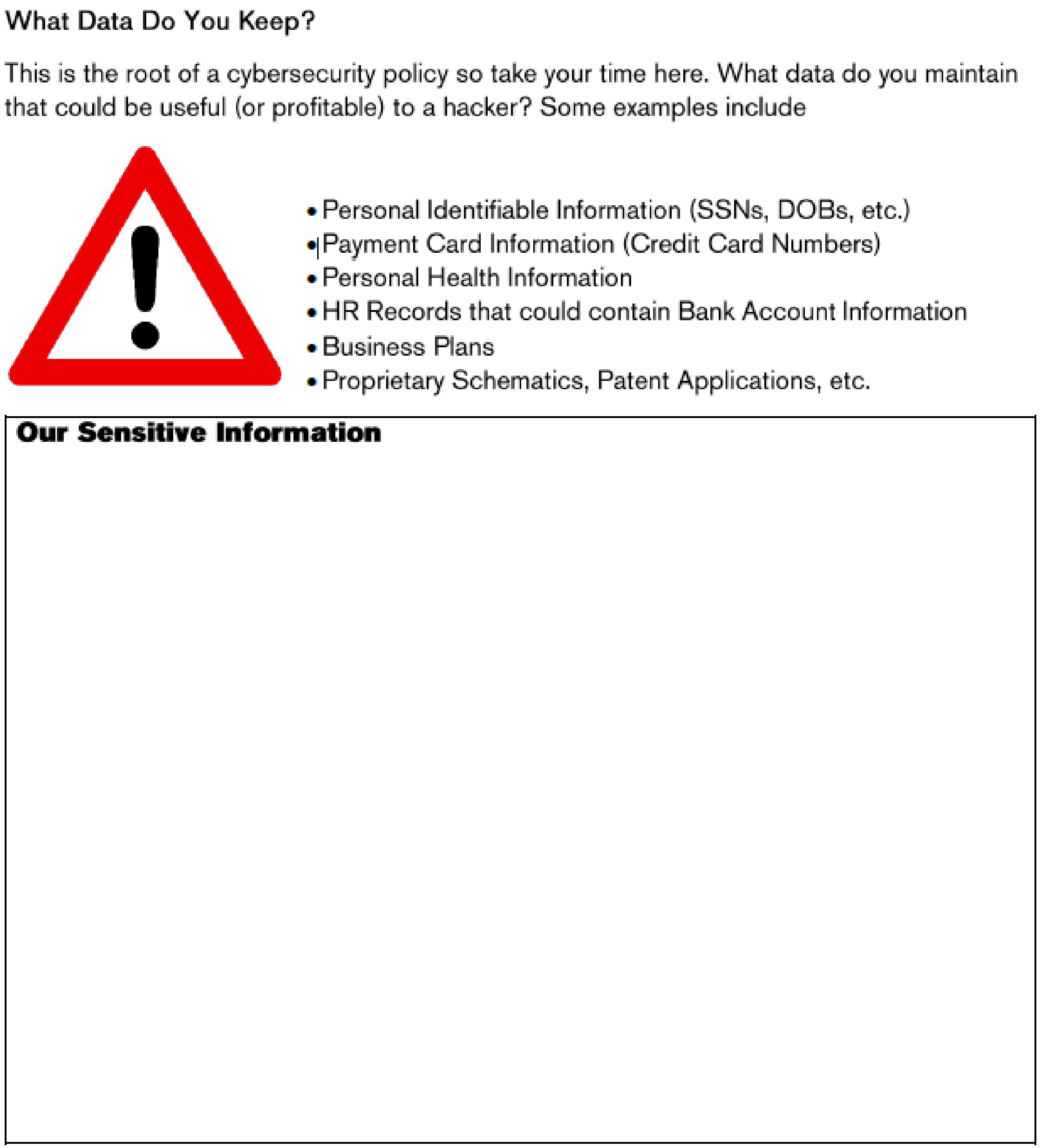


STEP 1 IDENTIFY	What structures and practices do you have in place to identify cyber threats? *PAGE 8*
STEP 2 PROTECT	What are the basic practices you have in place to protect your systems? *PAGE 12*
STEP 3 DETECT	What do you use to identify someone or something malicious? *PAGE 19*
STEP 4 RESPOND	How will you deal with a breach if and when it occurs? *PAGE 21*
STEP 5 RECOVER	How will you get your business back to normal after a breach? *PAGE 23*

STEP 1
IDENTIFY

Other pieces of the Identify section:

- Who is responsible for cybersecurity in my organization?
- What devices need protecting?
- What operating systems are you using?
- Where do I store my data?



What Data Do You Keep?

This is the root of a cybersecurity policy so take your time here. What data do you maintain that could be useful (or profitable) to a hacker? Some examples include

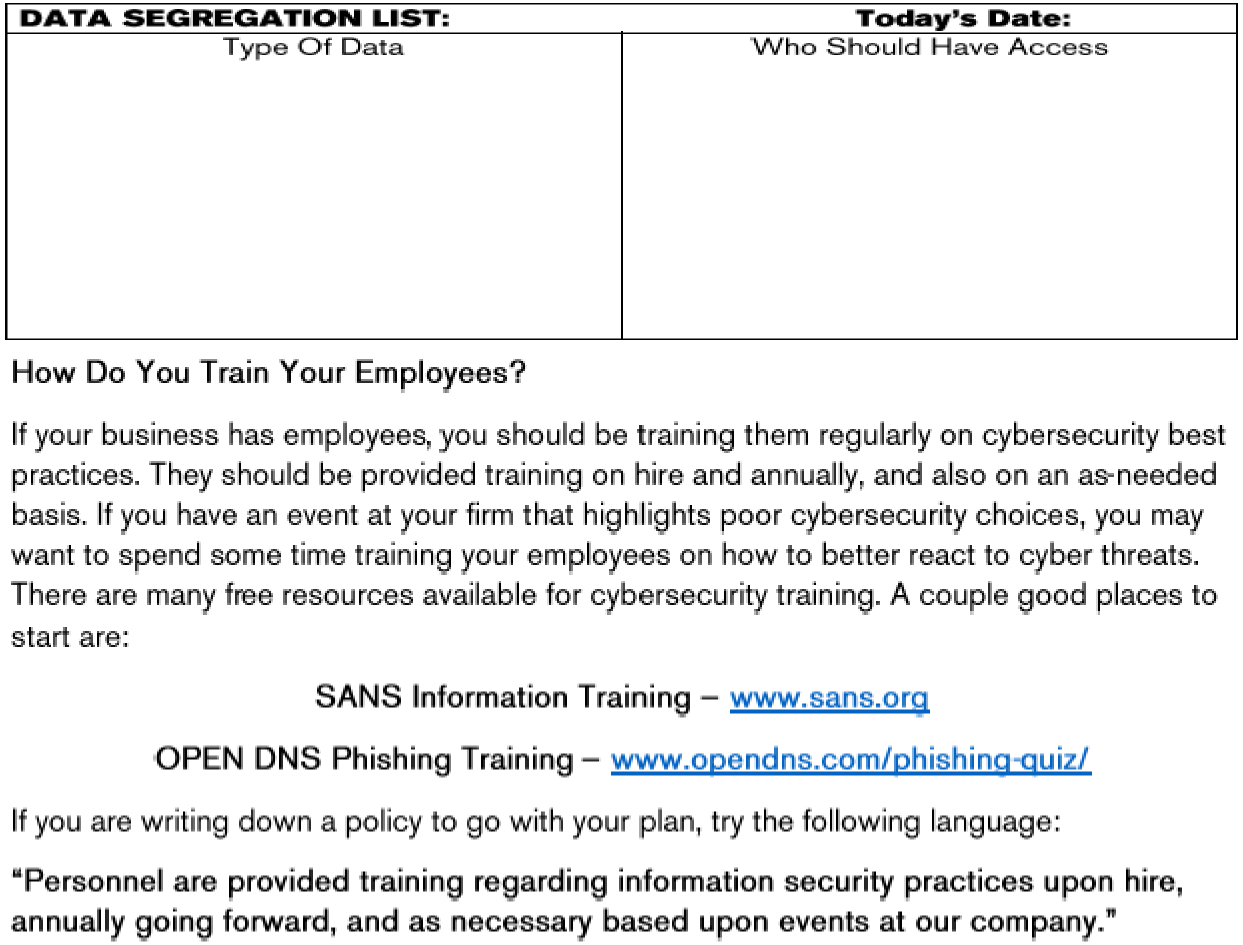
- Personal Identifiable Information (SSNs, DOBs, etc.)
- Payment Card Information (Credit Card Numbers)
- Personal Health Information
- HR Records that could contain Bank Account Information
- Business Plans
- Proprietary Schematics, Patent Applications, etc.

Our Sensitive Information

STEP 2
PROTECT

Other pieces of the Protect section:

- How do you use firewalls?
- Encryption checklist
- Accessing files remotely
- Username check
- Password check
- *Note, Identify and Protect sections are larger than last 3



DATA SEGREGATION LIST:	**Today's Date:**
Type Of Data	Who Should Have Access

How Do You Train Your Employees?

If your business has employees, you should be training them regularly on cybersecurity best practices. They should be provided training on hire and annually, and also on an as-needed basis. If you have an event at your firm that highlights poor cybersecurity choices, you may want to spend some time training your employees on how to better react to cyber threats. There are many free resources available for cybersecurity training. A couple good places to start are:

SANS Information Training – www.sans.org

OPEN DNS Phishing Training – www.opendns.com/phishing-quiz/

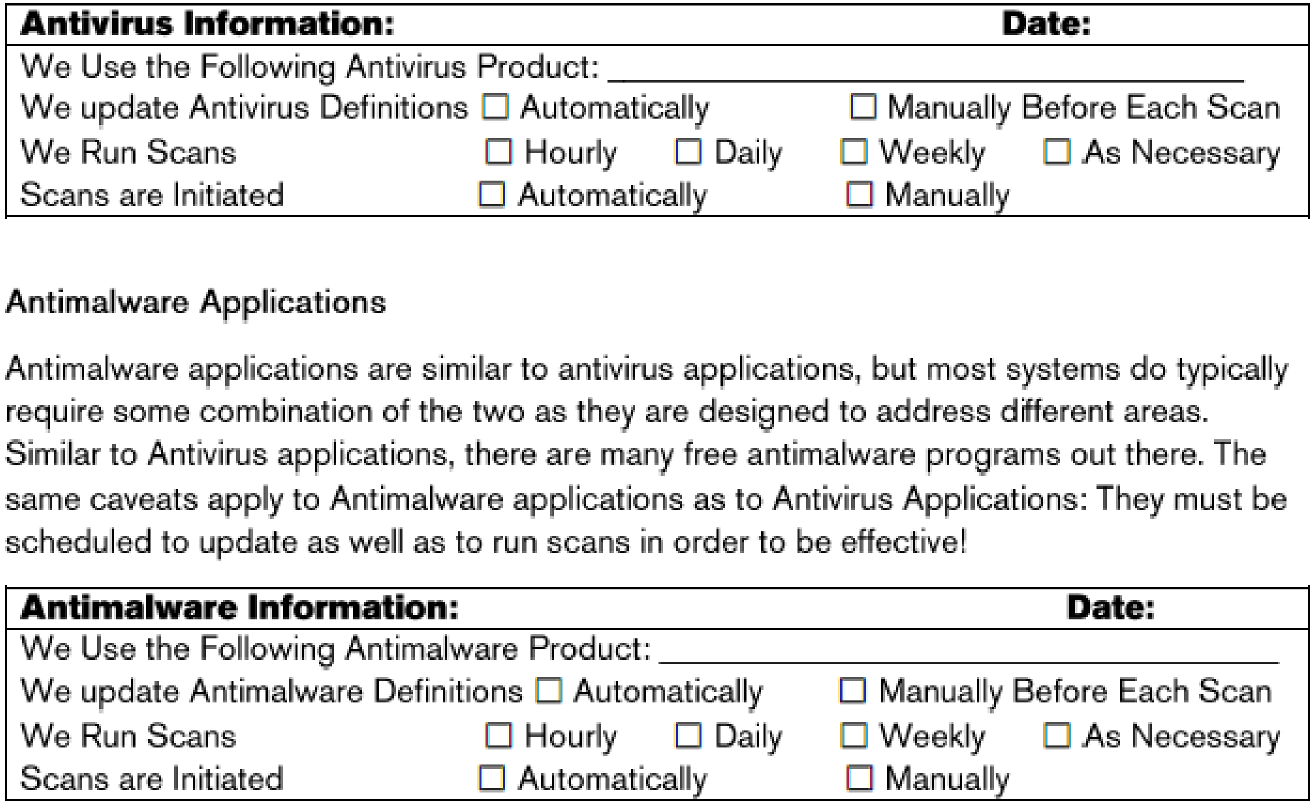
If you are writing down a policy to go with your plan, try the following language:

"Personnel are provided training regarding information security practices upon hire, annually going forward, and as necessary based upon events at our company."

STEP 3
DETECT

Other pieces of the Detect section:

- Determining the Impact of an event
- More complex methods detection



Antivirus Information: **Date:**

We Use the Following Antivirus Product: ____________________

We update Antivirus Definitions □ Automatically □ Manually Before Each Scan

We Run Scans □ Hourly □ Daily □ Weekly □ As Necessary

Scans are Initiated □ Automatically □ Manually

Antimalware Applications

Antimalware applications are similar to antivirus applications, but most systems do typically require some combination of the two as they are designed to address different areas. Similar to Antivirus applications, there are many free antimalware programs out there. The same caveats apply to Antimalware applications as to Antivirus Applications: They must be scheduled to update as well as to run scans in order to be effective!

Antimalware Information: **Date:**

We Use the Following Antimalware Product: ____________________

We update Antimalware Definitions □ Automatically □ Manually Before Each Scan

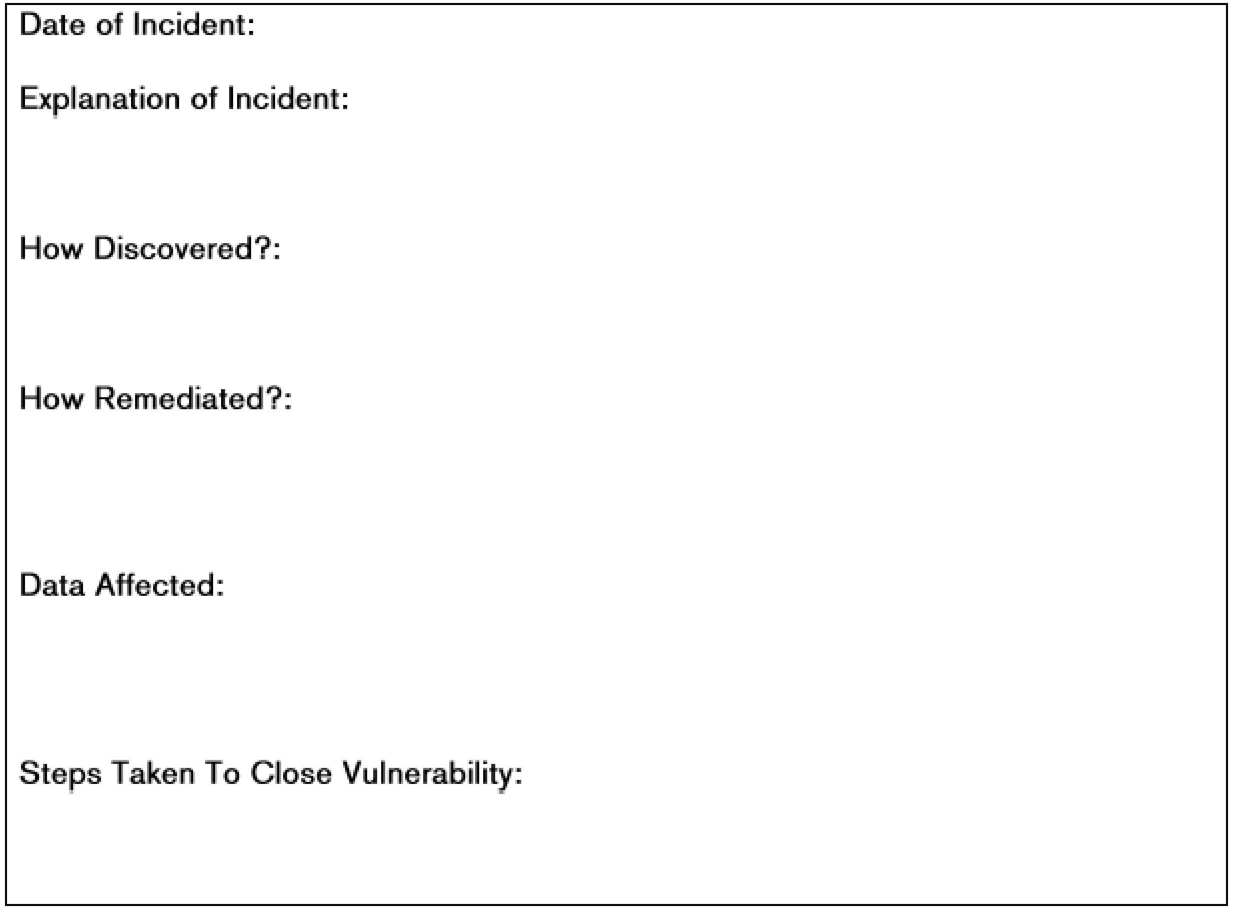
We Run Scans □ Hourly □ Daily □ Weekly □ As Necessary

Scans are Initiated □ Automatically □ Manually

STEP 4
RESPOND

Other pieces of the Respond section:

- Incorporating Lessons Learned
- Data Backup
- Digital Forensics Contact
- Containing an event



Date of Incident:

Explanation of Incident:

How Discovered?:

How Remediated?:

Data Affected:

Steps Taken To Close Vulnerability:

STEP 5
RECOVER

Other pieces of the Recover section:

- Customized with state-specific information
- Coming soon, a list of local cyber specialists, lawyers, insurance agents, state agencies, and educational opportunities.

Who are your resources?

Before a breach identify what resources you will need to help you in the event of a serious IT security event or one which involved client/sensitive information.

In the event of a breach your first call should likely be to legal support, an attorney with knowledge of breach response and remediation. Again, you need not put an attorney on retainer, but knowing who you are going to call before you need them will save valuable time in the event of a breach. Identify your legal resources now!

You may also wish to consider identifying your local police resources who may be of assistance.

Tips For Small Businesses

DATASSURED™

Top Ten Cybersecurity Tips for Your Small Business

Protect against, viruses, spyware and other malicious code

- Equip computers with antivirus software and antispyware and update regularly. Configure them to update automatically.

Secure your networks

- Safeguard your Internet connection by using a firewall and by encrypting information. Hide and secure your Wi-Fi network and password protect access to your router.

Establish security practices and policies

- Establish policies for how employees should handle and protect sensitive data, and clearly outline consequences for violating your business' cyber policies.

Educate employees about cyber threats

- Teach employees how to protect your business' data, including safe use of social networking sites and email

Require employees to use strong passwords

- Consider implementing multifactor authentication that requires additional information beyond a password to gain entry.

Employ best practices on payment cards

- Isolate payment systems from other less secure systems and do not use the same computer to process payments and surf the internet.

Make backup copies of important business data

- Regularly backup the data on all computers, and try to do it automatically, if possible, and store the copies either offsite or on the cloud.

Control physical access to computers and networks

- Prevent access or use of business computers by unauthorized individuals.

Create a mobile device action plan

- Require users to password protect all devices, encrypt their data, and install security apps to prevent criminals from stealing information. Set reporting procedures for lost or stolen equipment.

Protect all pages on your public-facing website

- Make security a priority for your entire digital foot-print.

Additional Resources

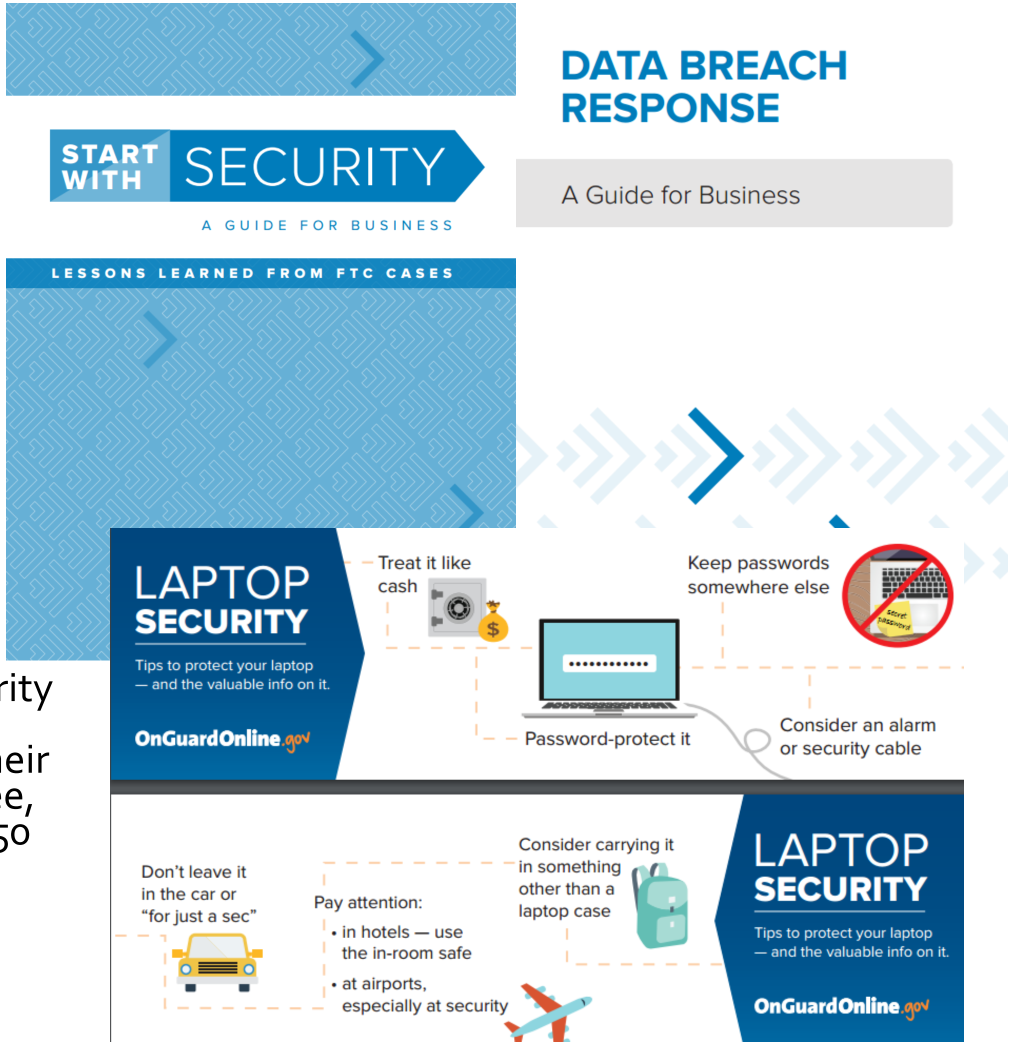
- Federal Trade Commission
  - FTC Bulk Order

- Payment Card Industry Small Merchant Task Force, PCI Security Standards Council Handouts
  - Small Merchant Guide to Safe Payments
  - Small Merchant Questions to Ask Your Vendors

- SANS Institute
  - Information Security Policy Templates

- National Cyber Security Alliance
  - https://staysafeonline.org/

- U.S. Small Business Administration & Synergy Solutions
  - launched a free, new comprehensive series of web-based cybersecurity training containing up to 10 modules to educate 7(j) eligible small businesses about cybersecurity and steps they can take to protect their company's assets and intellectual property. While the classes are free, they are first come, first serve and will accommodate no more than 50 participants at a time. To register, visit: https://synergysolutions.talentlms.com/.


START WITH SECURITY
A GUIDE FOR BUSINESS
LESSONS LEARNED FROM FTC CASES
DATA BREACH RESPONSE
A Guide for Business
LAPTOP SECURITY
Tips to protect your laptop — and the valuable info on it.
OnGuardOnline.gov
Treat it like cash
Keep passwords somewhere else
Password-protect it
Consider an alarm or security cable
Don't leave it in the car or "for just a sec"
Pay attention:
• in hotels — use the in-room safe
• at airports, especially at security
Consider carrying it in something other than a laptop case
LAPTOP SECURITY
Tips to protect your laptop — and the valuable info on it.
OnGuardOnline.gov

AMERICA'S SBDC KANSAS CYBER

Brian S. Dennis
Director
Cybersecurity Center
for Small Business
785-864-0286
Brian.dennis@ku.edu