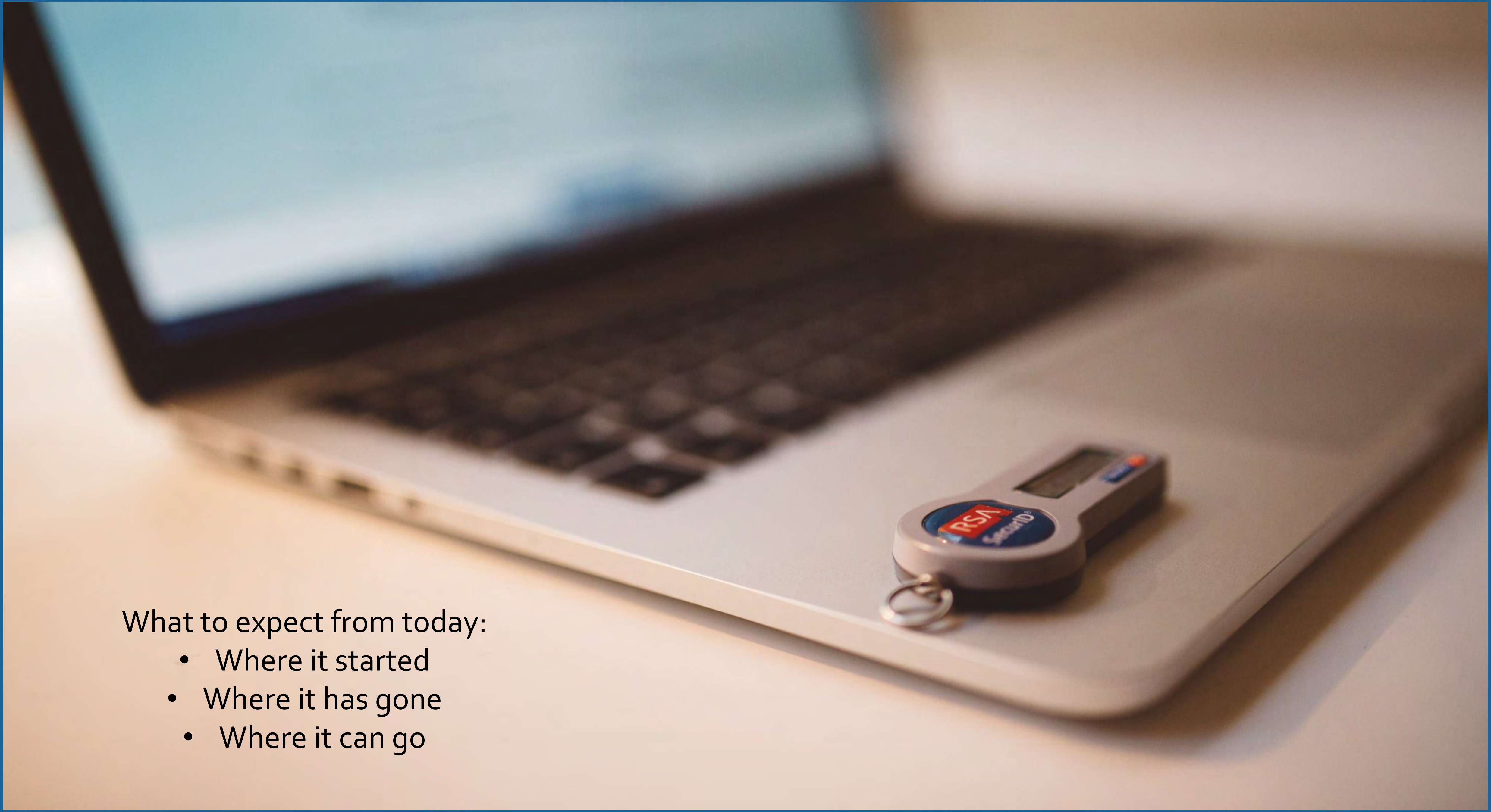
Bridging the Gap:
Bringing Free Cyber Security Education to America’s Small Businesses

Brian S. Dennis
Director
Cybersecurity Center for Small Business
Kansas Small Business Development Center



What to expect from today:

- Where it started
- Where it has gone
- Where it can go

Brian S. Dennis

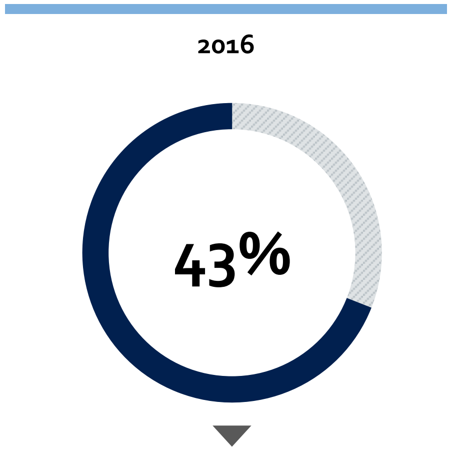
- Frontline Experience in Disaster Response and Recovery
  - Hurricane Katrina 2005
  - Hurricane Rita 2005
  - Hurricane Gustav 2008
  - Hurricane Ike 2008
- Disaster Recovery Institute International Certification
  - ABCP 2014- Present
    - Certification #: 44083
- Masters of Emergency Management & Homeland Security
  - Arizona State University, 12/2017

2017 National Defense Authorization Act

IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Small Business Administration and the Secretary of Homeland Security shall work collaboratively to develop a cyber strategy for small business development centers to be known as the ''Small Business Development Center Cyber Strategy''.

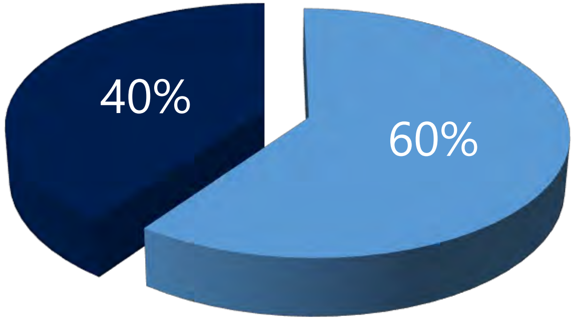
Small Businesses are a Target

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….



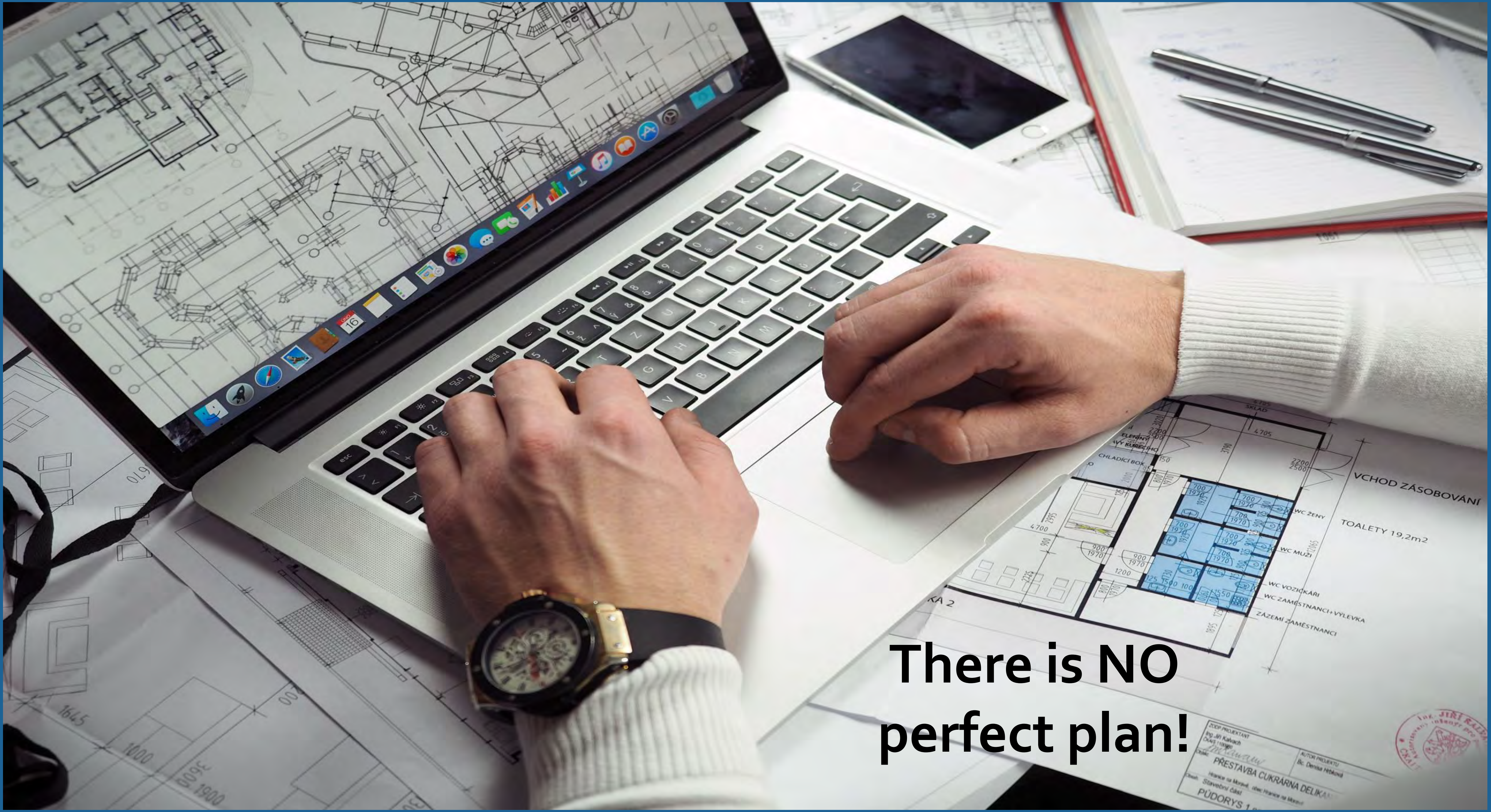
PCWorld in August 2013 reported that of the small businesses who suffered a breach, roughly 60 percent go out of business within six months after the attack.

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

Simple Solution to a Difficult Problem: Cast a Wide Net



There is NO perfect plan!

- Raise awareness of cyber risk within America’s small business community.
- Help businesses manage the threat and impact of cyber interference.
- Foster innovation in cyber security

Cyber Program Elements

Industry-Specific Training

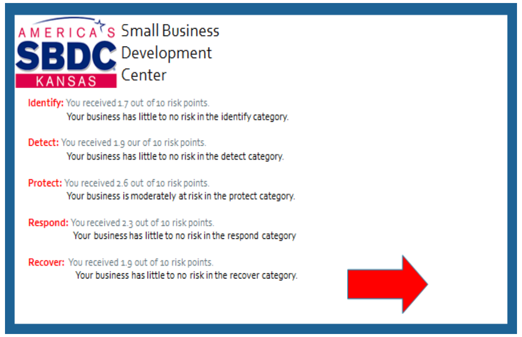
ASBDC Advisor Development

AMERICA'S SBDC KANSAS

Fostering Innovation

SBIR · STTR America's Seed Fund

Custom Small Business Resources



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

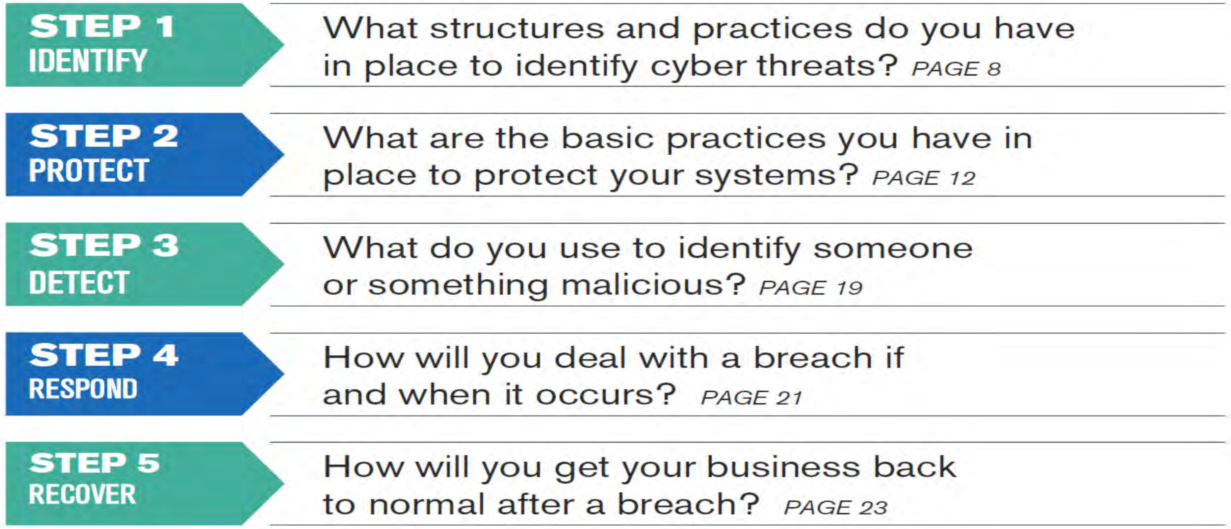
Recover: You received 1.9 out of 10 risk points.
Your business has little to no risk in the recover category.

- 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*

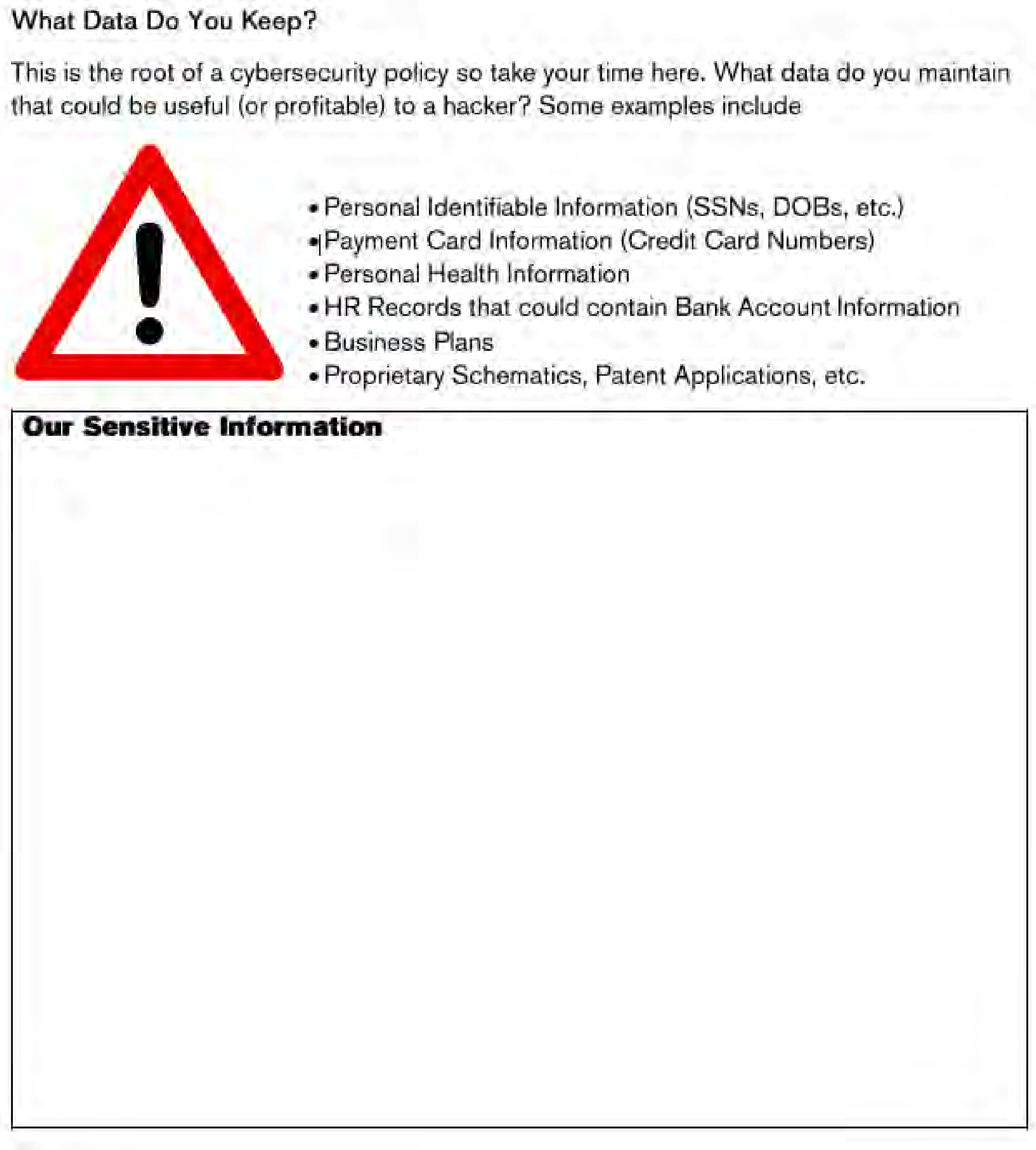
STEP 4 RESPOND How will you deal with a breach if and when it occurs? *PAGE 21*

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

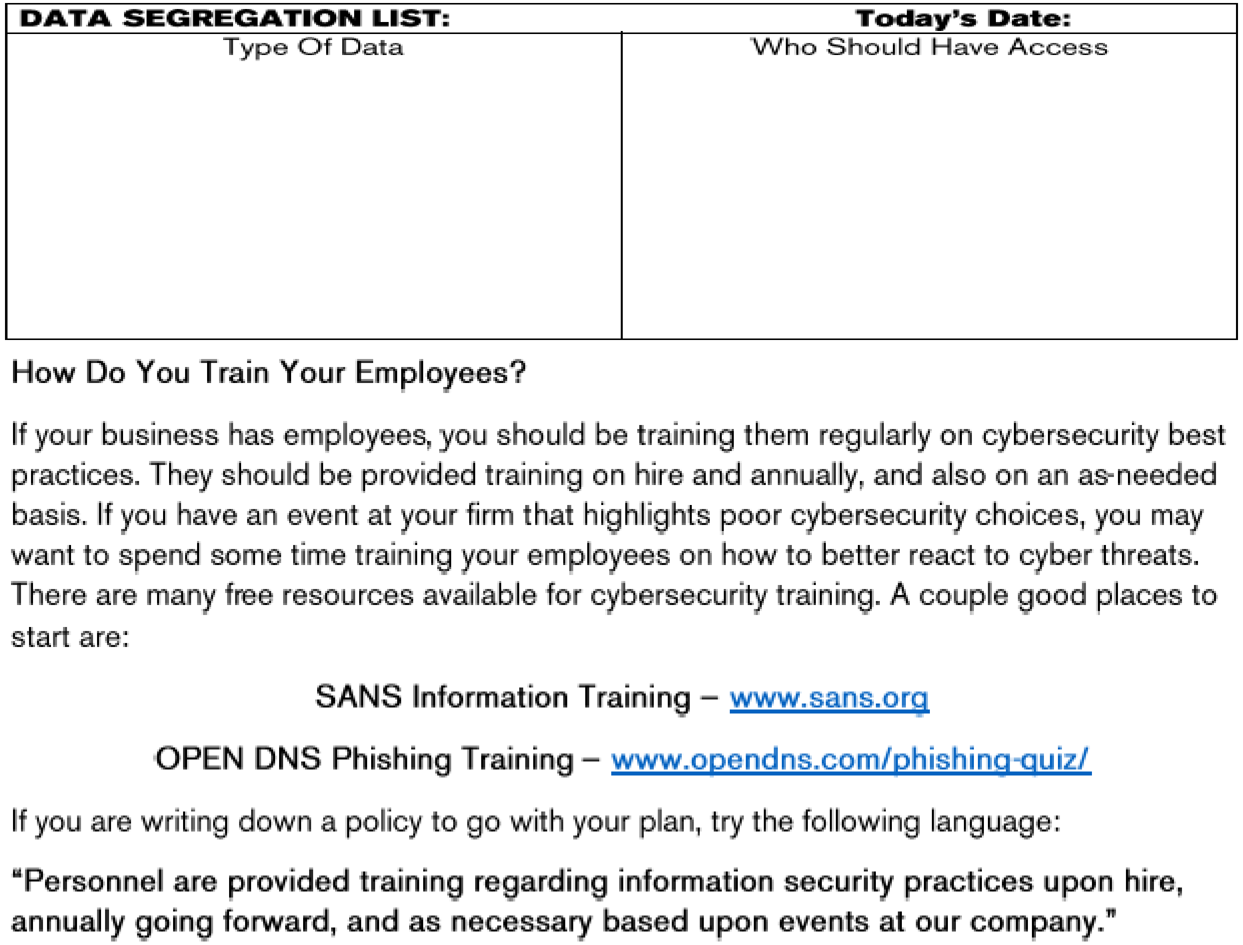
- Personal Identifiable Information (SSNs, DOBs, etc.)
- Payment Card Information (Credit Card Numbers)
- Personal Health Information
- HR Records that could contain Bank Account Information
- Business Plans
- Proprietary Schematics, Patent Applications, etc.

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/

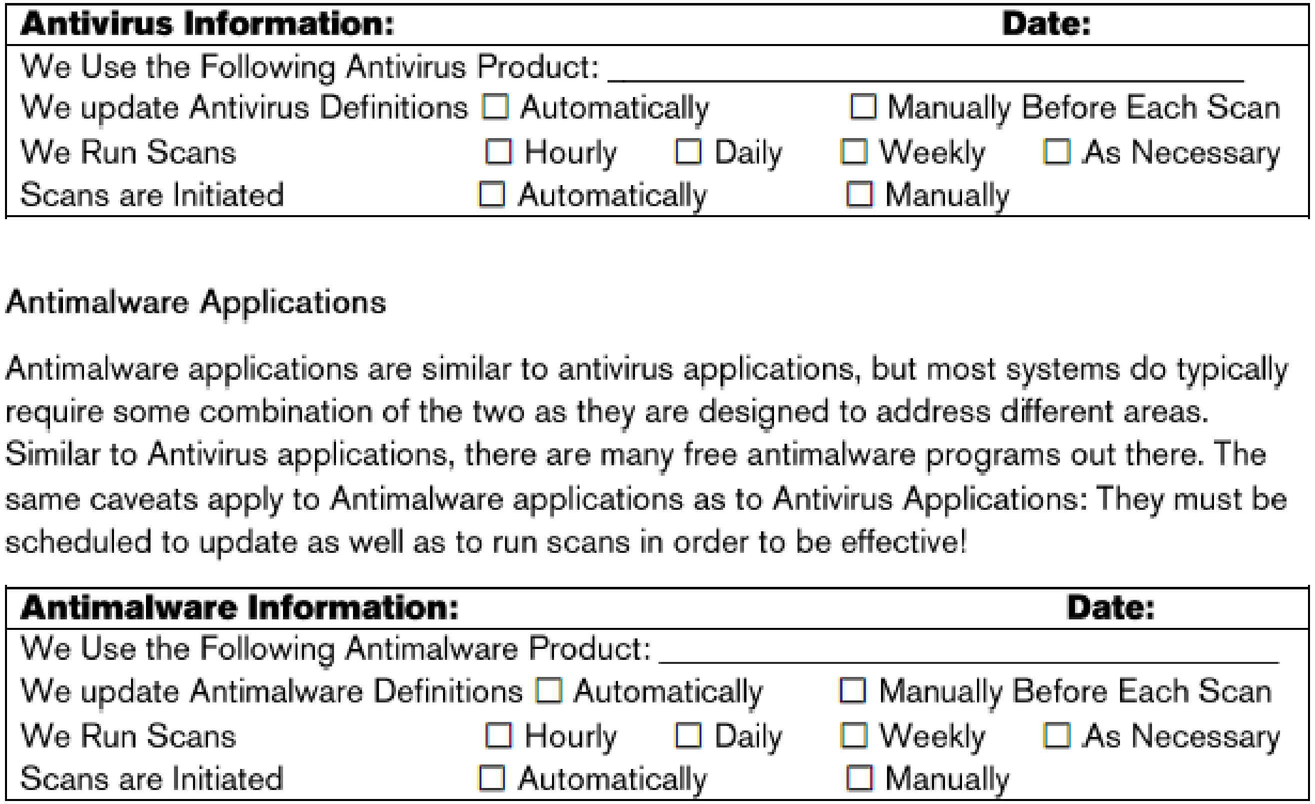
If you are writing down a policy to go with your plan, try the following language:

"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

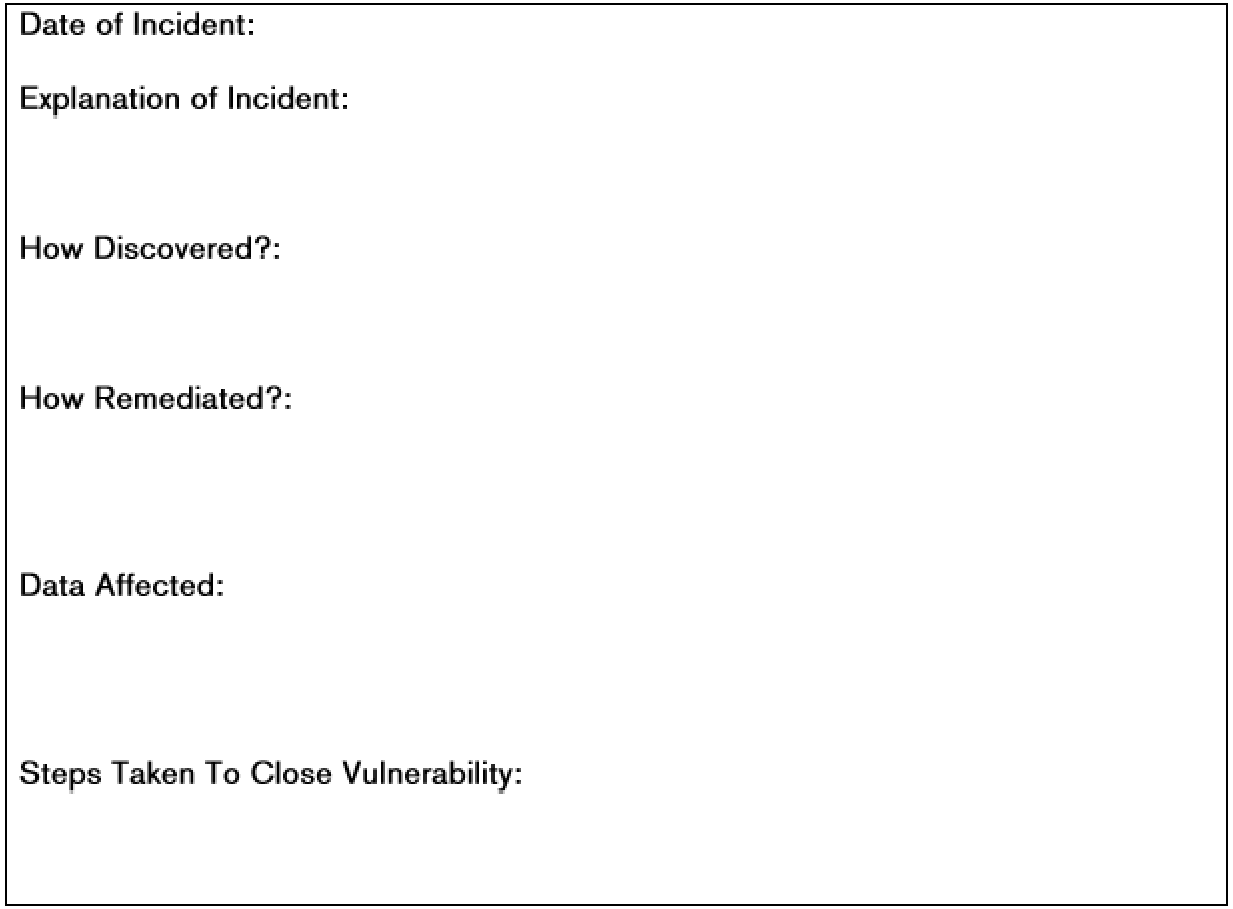
We Run Scans □ Hourly □ Daily □ Weekly □ As Necessary

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

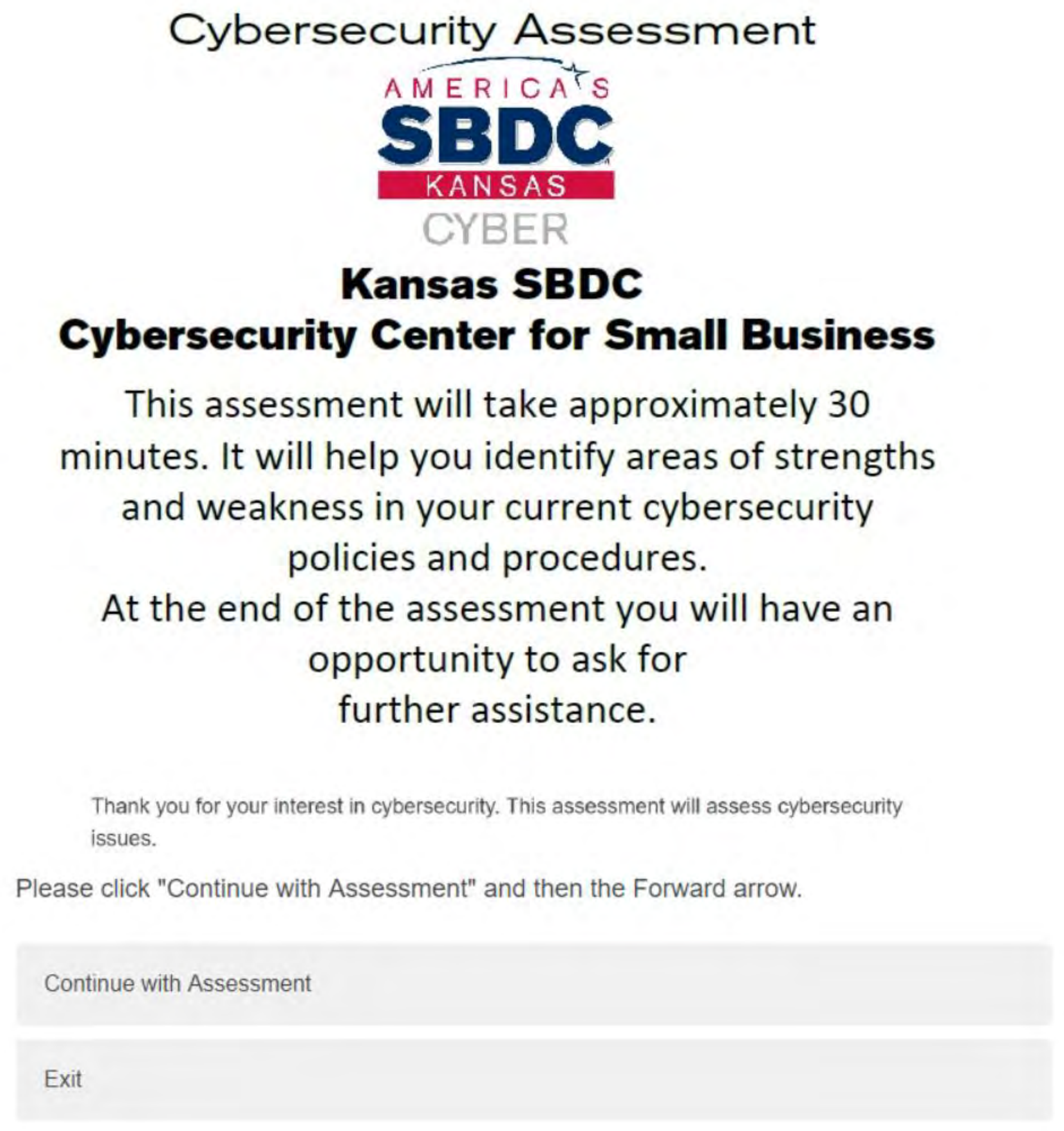
- Coming soon, a list of local cyber specialists, lawyers, insurance agents, state agencies, and educational opportunities.

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.



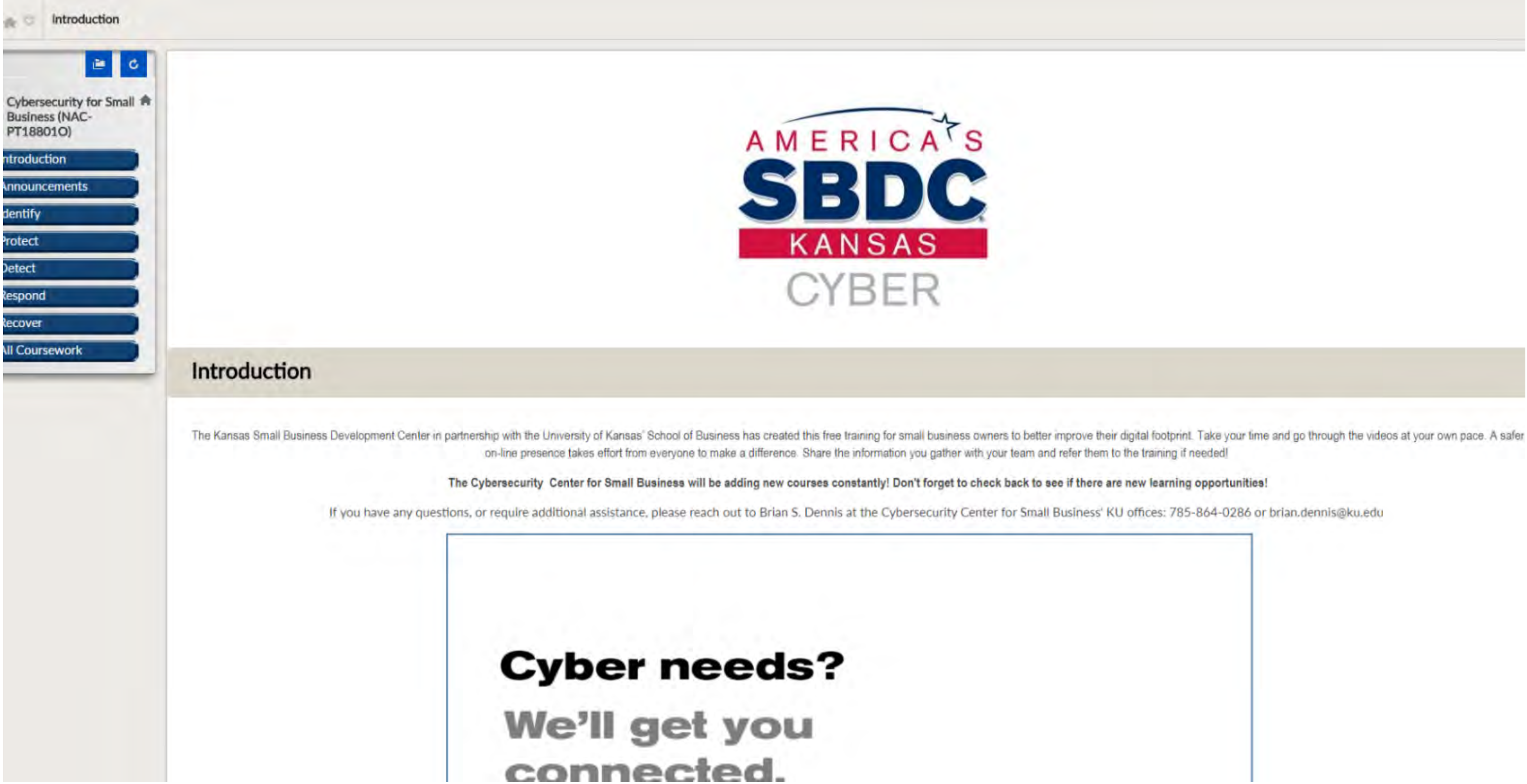
Cybersecurity Assessment

Kansas SBDC
Cybersecurity Center for Small Business

This assessment will take approximately 30 minutes. It will help you identify areas of strengths and weakness in your current cybersecurity policies and procedures.
At the end of the assessment you will have an opportunity to ask for
further assistance.

Thank you for your interest in cybersecurity. This assessment will assess cybersecurity issues.

Please click "Continue with Assessment" and then the Forward arrow.



Introduction

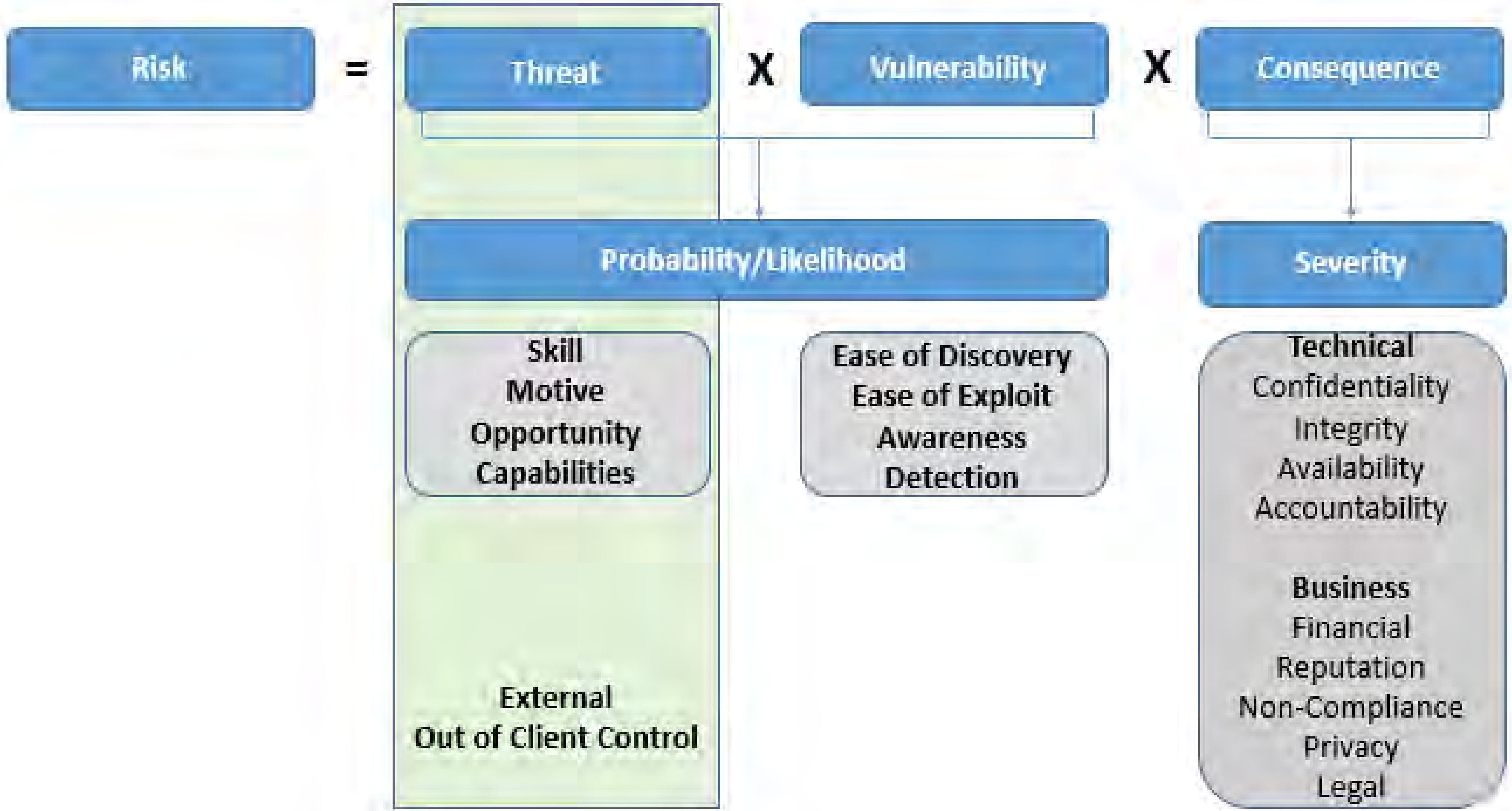
The Kansas Small Business Development Center in partnership with the University of Kansas' School of Business has created this free training for small business owners to better improve their digital footprint. Take your time and go through the videos at your own pace. A safer on-line presence takes effort from everyone to make a difference. Share the information you gather with your team and refer them to the training if needed!

The Cybersecurity Center for Small Business will be adding new courses constantly! Don't forget to check back to see if there are new learning opportunities!

If you have any questions, or require additional assistance, please reach out to Brian S. Dennis at the Cybersecurity Center for Small Business' KU offices: 785-864-0286 or brian.dennis@ku.edu

Cyber needs?

We'll get you connected.



Risk = Threat X Vulnerability X Consequence

Probability/Likelihood

Severity

Skill
Motive
Opportunity
Capabilities

Ease of Discovery
Ease of Exploit
Awareness
Detection

Technical
Confidentiality
Integrity
Availability
Accountability

Business
Financial
Reputation
Non-Compliance
Privacy
Legal

External
Out of Client Control

- Assessments are updated regularly
- Training modules (45 by the end of 2018) can be created quickly with immediate launch into portal
- Client usage from the assessment to the training will be tracked via a CRM that can move data to Neoserra/CenterIC—allowing for a true virtual center to exist in an SBDC network

Time to Grow

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