Kentucky Nonprofits & COVID-19 – Sector Resources
Cybersecurity in a Pandemic for Small Businesses

All participants have been automatically muted.

During today’s conversation, if you would like to submit a question, please use the “CHAT” feature located at the bottom of your Zoom screen.

You can also find COVID-19 resources on www.kynonprofits.org

We will begin the program shortly.
Cybersecurity in a Pandemic

Jason D. Miller
Director, Business & Technology Consulting
Agenda

1. Small business cybersecurity pre-pandemic
2. Rush to work from home
3. Cybersecurity during a pandemic
4. Online meeting tools discussion
5. Cybersecurity post-pandemic
Small Business Cybersecurity Pre-Pandemic
Industry reports

2019 Data Breach Investigations Report

Exclusive Research Report
2019 Global State of Cybersecurity in Small and Medium-Sized Businesses
Sponsored by Keeper Security, Inc.
Independently conducted by Ponemon Institute LLC
Small Business Prime Targets

- 16% were breaches of Public sector entities
- 15% were breaches involving Healthcare organizations
- 10% were breaches of the Financial industry
- 43% of breaches involved small business victims

Figure 2. Who are the victims?
What tactics are utilized?

- 52% of breaches featured Hacking
- 33% included Social attacks
- 28% involved Malware
- Errors were causal events in 21% of breaches
- 15% were Misuse by authorized users
- Physical actions were present in 4% of breaches
Top hacking actions?
What are other commonalities?

- 71% of breaches were financially motivated
- 25% of breaches were motivated by the gain of strategic advantage (espionage)
- 32% of breaches involved phishing
- 29% of breaches involved use of stolen credentials
- 56% of breaches took months or longer to discover
Small Business with Cyberattacks

Figure 1. Our company experienced a cyberattack and data breach in the past 12 months
Yes responses

<table>
<thead>
<tr>
<th></th>
<th>FY2017</th>
<th>FY2018</th>
<th>FY2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyberattack</td>
<td>61%</td>
<td>67%</td>
<td>66%</td>
</tr>
<tr>
<td>Data breach</td>
<td>54%</td>
<td>58%</td>
<td>63%</td>
</tr>
</tbody>
</table>
Why aren’t small businesses better at cybersecurity?
Cost of a breach and business disruption?
The Rush to Work From Home
March 2020
What did we see happen in a matter of days?

### Remote Access?
- Open up remote desktop services
- More VPN users
- Third-party tools (free?)

### Who?
- Untrained users
- Employees out of their comfort zone

### Devices?
- Grab any spare laptop
- Employee's home computers

### Communication?
- Free video conferencing
- Personal email
- Personal file shares
Concerns created by the rush

Remote Access?
What new vulnerabilities did you just open up for cyber criminals to access your network?

Who?
Are your users really prepared? Users are our number one vulnerability is cybersecurity.

Devices?
How many vulnerable and unpatched devices are processing your critical data?

Communication?
Where is your sensitive information going?
Cybersecurity During the Pandemic
Do it NOW

- **Remote access**: Make sure NO open RDP, Secure all remote - MFA
- **Get devices updated**: Swap out all old devices with patched and secure
- **Secure password policies**: Review and implement secure password policies
- **External vulnerability scan**: Have a professional do a quick external scan
Online Meeting Tools
Popular tools and recent news

Best Practices

- Use unique meeting ID’s for each meeting
- Require a password or ping to gain access to meetings
- Privately share meeting invitations.
- Consider requiring users to enable the “Lobby” or “Waiting room” functionality and affirming entry into a meeting.
- If your users are using client-applications versus the web interface, be sure the client applications are updated frequently to gain any security patches and enhancements that are released.
Cybersecurity Post-Pandemic
Key cybersecurity considerations

Do you have the right protection tools?

Have you had a third-party Cyber assessment conducted? Recently?

Does your organization conduct regular user awareness training?

Would you know if your systems have been compromised? Do you have monitoring tools?
Information Security Program

PEOPLE

TECHNOLOGY

PROCESSES
People

52% of breaches featured Hacking
33% included Social attacks
28% involved Malware
Errors were causal events in 21%
15% were Misuse by authorized
Physical actions were present in

Breaches

Figure 3. What tactics are utilized?

User Awareness

It is critical to train and equip our users on the frontlines.

KnowBe4
Human error. Conquered.

Figure 12. Top threat action varieties in breaches (n=1714)
Processes & Controls

Risk Assessment
- Not just a technology exercise
- Must be continual

Information Security Program
- Policies and Procedures
- User education
- Technology
- Roadmap for improvement

Monitoring & Response
- Tools to monitor and provide early detection
- Incident Response plans

Business Continuity
- Documentation & planning
- Strong and reliable backups
Assessment: Dean Dorton Cybersecurity Scorecard

External Security Review (EXT)
Risk level associated with your internet facing assets. Threats include direct, technical attacks, and credential theft.

Overall Organizational Risk
Overall organization risk based upon an average of the four areas evaluated.

Endpoint Security Review (ESR)
Risk level associated with your internal workstations and servers. Threats include exploitation and malware infection.

Common Controls Review (CCR)
Risk level associated with implementation of shared, organizational cyber-security controls.
Security Lifecycles

Small Business Model

1. Cybersecurity Scorecard Assessment
2. Onboarding Activities
   - Security policy and acceptable use policy
   - Incident response process
   - Security awareness
   - Remediaion (optional service)
   - Incident response (optional service)
3. Ongoing Activities
   - Quarterly cybersecurity assessment
   - Monthly security log reviews
   - Security awareness and industry trends

Large to Medium Model

1. Program Maturity Review
2. Roadmap
   - Reporting
   - Incident Response
   - Technical Security Solutions
   - Security Monitoring
   - Security Awareness
   - Risk Assessment
   - Policies and Procedures
Technology

MFA
Multi-factor Authentication

Next-Gen
Anti-virus

Advanced
Web Filter

Advanced
Email Protection
Other considerations

**Office 365**
Have someone evaluate your **Office 365 security** and controls

**Remote Workforce**
- Should all users have a laptop?
- Virtual Desktop Solutions
- Cloud Solutions

**Passwords**
- Deploy a **password filter**
- Require strong passwords
- Minimum length 12
- Age: 180 days

**Backups**
- Multiple layers
- Air gap
- **Test** regularly
The one thing…

MFA
Multi-factor Authentication
Resources

deandorton.com/insights

deandorton.com/remote-work

deandorton.com/cybersecurity
What questions do you have?

Use the Chat box now
Thank you

Jason D. Miller
Director, Business & Technology Consulting
jmiller@ddaftech.com
859.425.7626