Cybersecurity Essentials for the New Year

*Webinar will begin promptly at 3pm Eastern
*All participants are muted
*Webinar is being recorded and will be made available after the event

www.staysafeonline.org

@staysafeonline
This was an excellent webinar with good information for small businesses and tech support companies like us who provide advice on support and security to our customers. The information covered can be passed along to our customers so they are #CyberAware!

Thanks to our National Sponsors

Signature Sponsor

Strategic Partner

TREND MICRO™ education

ITSP MAGAZINE™

Over 6,000 webinar attendees

Over 5,000 workshop attendees

Over 15,000 subscribers
Today’s Guest Speaker

Kevin Dillon
Associate Director, Strategic Relations,
Stakeholder Engagement Division,
Cybersecurity and Infrastructure Security Agency (CISA)

https://www.cisa.gov
Cybersecurity and Infrastructure Security Agency (CISA)

VISION
Secure and resilient infrastructure for the American people.

MISSION
Lead the Nation’s efforts to understand and manage risk to our critical infrastructure.
THE LEADER'S GUIDE

Reducing your organization's cyber risks requires a holistic approach - similar to the approach you would take to address other operational risks. As with other risks, cyber risks can threaten:

- Your ability to operate/access info
- Your reputation/customer trust
- Your bottom line
- Your organization's survival

Managing cyber risks requires building a culture of cyber readiness.

Essential Elements of a Culture of Cyber Readiness:

**Yourself** - The Leader

- Drive cybersecurity strategy, investment and culture

  Your awareness of the basics drives cybersecurity to be a major part of your operational resilience strategy, and that strategy requires an investment of time and money. Your investment drives actions and activities that build and sustain a culture of cybersecurity.

**Your Staff** - The Users

- Develop security awareness and vigilance

  Your staff will often be your first line of defense, one that must have and continuously grow the skills to practice and maintain readiness against cybersecurity risks.

**Your Systems** - What Makes You Operational

- Protect critical assets and applications

  Information is the life-blood of any business; it is often the most valuable of a business' intangible assets. Know where this information resides, know what applications and networks store and process that information, and build security into and around these.

**Your Surroundings** - The Digital Workplace

- Ensure only those who belong on your digital workplace have access

  The authority and access you grant employees, managers, and customers into your digital environment needs limits, just as those in the physical workplace do. Setting approved access privileges requires knowing who operates on your systems and with what level of authorization and accountability.

**Your Data** - What the Business is Built On

- Make backups and avoid the loss of information critical to operations

  Even the best security measures can be circumvented with a patient, sophisticated adversary. Learn to protect your information where it is stored, processed, and transmitted. Have a contingency plan, which generally starts with being able to recover systems, networks, and data from known, accurate backups.

**Your Actions Under Stress**

- Limit damage and quicken restoration of normal operations

  The strategy for responding to and recovering from compromise plans, prepare for, and conduct drills for cyberattacks as you would a fire. Make your reaction to cyberattacks and system failures an extension of your other business contingency plans. This requires having established procedures, trained staff, and knowing how and to whom to communicate during a crisis.

CISA.gov/Cyber-Essentials
**THE IT PROFESSIONAL’S GUIDE**

Essential Actions for Building a Culture of Cyber Readiness:

<table>
<thead>
<tr>
<th>Yourself</th>
<th>Your Staff</th>
<th>Your Systems</th>
<th>Your Surroundings</th>
<th>Your Data</th>
<th>Your Actions Under Stress</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Develop a cybersecurity strategy, investment, and culture.</td>
<td>- Develop security awareness and vigilance.</td>
<td>- Protect critical assets and applications.</td>
<td>- Ensure only those who belong on your digital workplace have access.</td>
<td>- Learn what information resides on your network. Maintained inventories of network connections (user accounts, vendors, business partners, etc.).</td>
<td>- Lead development of an incident response and disaster recovery plan outlining roles and responsibilities. Test it often.</td>
</tr>
<tr>
<td>- Understand how much of their operations are dependent on IT.</td>
<td>- Built a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information.</td>
<td>- Identified available training resources through professional associations, academic institutions, private sector, and government sources.</td>
<td>- Secured systems and data from unauthorized access.</td>
<td>- Leveraged secure multi-factor authentication for all users, starting with privileged, administrative and remote access accounts.</td>
<td>- Leveraged business impact assessments to identify resources and identify which systems must be recovered first.</td>
</tr>
<tr>
<td>- Approached cyber as a business risk.</td>
<td>- Lead development of cybersecurity policies.</td>
<td>- Leveraged automatic updates for all operating systems and third-party software.</td>
<td>- Secured systems and data from unauthorized access.</td>
<td>- Leveraged secure multi-factor authentication for all users, starting with privileged, administrative and remote access accounts.</td>
<td>- Leveraged business impact assessments to identify resources and identify which systems must be recovered first.</td>
</tr>
<tr>
<td>- Develop a culture of awareness to encourage employees to make good choices online.</td>
<td>- Leveraged basic cybersecurity training to improve exposure to cybersecurity concepts, terminology, and activities associated with implementing cybersecurity best practices.</td>
<td>- Leveraged secure multi-factor authentication for all users, starting with privileged, administrative and remote access accounts.</td>
<td>- Secured systems and data from unauthorized access.</td>
<td>- Leveraged backup and disaster recovery plans, including offsite storage of critical data.</td>
<td>- Leveraged business impact assessments to identify resources and identify which systems must be recovered first.</td>
</tr>
<tr>
<td>- Learn about risks like phishing and business email compromise.</td>
<td>- Identified available training resources through professional associations, academic institutions, private sector, and government sources.</td>
<td>- Leveraged secure multi-factor authentication for all users, starting with privileged, administrative and remote access accounts.</td>
<td>- Secured systems and data from unauthorized access.</td>
<td>- Leveraged business impact assessments to identify resources and identify which systems must be recovered first.</td>
<td>- Leveraged business impact assessments to identify resources and identify which systems must be recovered first.</td>
</tr>
<tr>
<td>- Maintained awareness of current events related to cybersecurity, using lessons-learned and reported events to remain vigilant against the current threat environment and agile to cybersecurity trends.</td>
<td>- Leveraged automatic updates for all operating systems and third-party software.</td>
<td>- Leveraged secure multi-factor authentication for all users, starting with privileged, administrative and remote access accounts.</td>
<td>- Secured systems and data from unauthorized access.</td>
<td>- Leveraged business impact assessments to identify resources and identify which systems must be recovered first.</td>
<td>- Leveraged business impact assessments to identify resources and identify which systems must be recovered first.</td>
</tr>
<tr>
<td>- Created application integrity and whitelisting policies so that only approved software is allowed to load and operate on their systems.</td>
<td>- Leveraged automatic updates for all operating systems and third-party software.</td>
<td>- Leveraged secure multi-factor authentication for all users, starting with privileged, administrative and remote access accounts.</td>
<td>- Secured systems and data from unauthorized access.</td>
<td>- Leveraged business impact assessments to identify resources and identify which systems must be recovered first.</td>
<td>- Leveraged business impact assessments to identify resources and identify which systems must be recovered first.</td>
</tr>
</tbody>
</table>

**Consistent with the NIST Cybersecurity Framework and other standards, these actions are the starting point to Cyber Readiness. To learn more, visit CISA.gov/Cyber-Essentials.**
CISA Resources

- [https://www.cisa.gov](https://www.cisa.gov)
- [https://www.cisa.gov/cyber-essentials](https://www.cisa.gov/cyber-essentials)
- [https://www.us-cert.gov/report](https://www.us-cert.gov/report)
  - Report Incidents, Phishing, Malware, or Vulnerabilities
- CISA Insights: [https://www.cisa.gov/insights](https://www.cisa.gov/insights)
  - Informed by U.S. cyber intelligence and real-world events, each CISA Insight provides background information on particular cyber threats and the vulnerabilities they exploit, as well as a ready-made set of mitigation activities that non-federal partners can implement
- CISA Alerts: [https://www.us-cert.gov/ncas](https://www.us-cert.gov/ncas)
  - Analysis Reports
  - Alerts
  - Current Activity
  - Bulletins
Questions/Inquiries About Cyber Essentials?

cisaessentials@cisa.dhs.gov
COMMON CYBERSECURITY MISCONCEPTIONS FOR SMALL AND MEDIUM-SIZED ORGANIZATIONS

Employees empowered with the resources and knowledge to protect your organization from cyber threats is one of the best lines of defense you can have. Part of that training should involve breaking down often-quoted cybersecurity misconceptions.

<table>
<thead>
<tr>
<th>Misconception #1:</th>
<th>Misconception #2:</th>
<th>Misconception #3:</th>
<th>Misconception #4:</th>
<th>Misconception #5:</th>
</tr>
</thead>
</table>
| My data (or the data I have access to) is not valuable.  
All data is valuable.  
**Take Action:** Do an assessment of the data you create, collect, store, access, transmit and then classify all the data by level of sensitivity so you can take steps to protect it appropriately. | Cybersecurity is a technology issue.  
Cybersecurity is best approached with a mix of employee training, clear, accepted policies and procedures and implementation of current technologies.  
**Take Action:** Educate every employee on their responsibility for protecting sensitive information. | Cybersecurity requires a huge financial investment.  
Many efforts to protect your data require little or no financial investment.  
**Take Action:** Create and institute cybersecurity policies and procedures, restrict administrative and access privileges, enable multi-factor authentication and train employees to spot malicious emails. | Outsourcing to a vendor washes your hands of liability during a cyber incident.  
You have a legal and ethical responsibility to protect sensitive data.  
**Take Action:** Put data sharing agreements in place with vendors and have a trusted lawyer review. | Cyber breaches are covered by general liability insurance.  
Many standard insurance policies do not cover cyber incidents or data breaches.  
**Take Action:** Speak with your insurance representative to understand your coverage and what type of policy would best fit your organization’s needs. |

<table>
<thead>
<tr>
<th>Misconception #6:</th>
<th>Misconception #7:</th>
<th>Misconception #8:</th>
<th>Misconception #9:</th>
<th>Misconception #10:</th>
</tr>
</thead>
</table>
| Cyberattacks always come from external actors.  
Succinctly put: cyberattacks do not always come from external actors.  
**Take Action:** Identify potential cybersecurity incidents that can come from within the organization and develop strategies to minimize those threats. | Younger people are better at cybersecurity than others.  
Age is not directly correlated to better cybersecurity practices.  
**Take Action:** Before giving someone responsibility to manage your social media, website and network etc., train them on your expectations of use and cybersecurity best practices. | Compliance with industry standards is sufficient for a security strategy.  
Simply complying with industry standards does not equate to a robust cybersecurity strategy for an organization.  
**Take Action:** Use a robust framework such as the NIST Cybersecurity Framework, to manage cybersecurity risk. | Digital and physical security are separate things altogether.  
Do not discount the importance of physical security.  
**Take Action:** Develop strategies and policies to prevent unauthorized physical access to sensitive information and assets (e.g., control who can access certain areas of the office.) | New software and devices are secure when I buy them.  
Just because something is new, does not mean it is secure.  
**Take Action:** Ensure devices are operating with the most current software, change the manufacturer’s default password to a unique, secure passphrase and configure privacy settings prior to use. |

To view more detailed descriptions and associated resources for each misconception, visit staysafeonline.org/cybersecure-business

https://staysafeonline.org/resource/10-cybersecurity-misconceptions-smbs/
Upcoming Events

Check out our upcoming webinars & in-person events: [https://staysafeonline.org/event_category/cybersecure-my-business/](https://staysafeonline.org/event_category/cybersecure-my-business/)

A few webinar topics we have scheduled for 2020 include:

- Cybersecurity for government contractors
- Phishing, Vishing & Smishing
- Cybersecurity on the go for distributed workforces & telecommuters
- Digital Spring Cleaning


#PrivacyAware

Become a Champion. It’s FREE!

3 Twitter chats: January 23, 27 and February 11. Want to participate? Email: info@staysafeonline.org
CyberSecure
MY BUSINESS
PLAN. PROTECT. RESPOND.

Signature Sponsor
Trend Micro
www.trendmicro.com

Strategic Partner
ITSP Magazine
https://www.itspmagazine.com/

@staysafeonline
Info@staysafeonline

National Cyber Security Alliance
www.staysafeonline.org/cybersecure-business