



CyberSecurity Webcademy:
Make It Harder for Cyber Criminals to Get In

Presenters



Justin Krentz – Account
Executive in Pennsylvania



Tyler Lewan – Account
Executive in Colorado

Agenda



Summary of Session 2: Securing Your Environment



How to make it harder for cybercriminals to get In



What's next?

Summary of Session #1: The Basics

- Security Assessment**
- Staff**
- Spam Email**
- Passwords**



Summary of Session #2: Securing Your Environment

- ✓ **Computer Updates**
- ✓ **Log Management**
- ✓ **Firewalls**
- ✓ **Encryption**



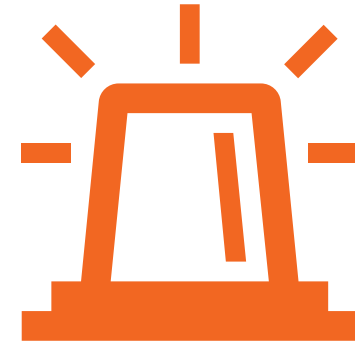
Risk #1: Rattling Your Digital Doors



- Any device is an entry point for threats
- A common weak spot that allow these attacks access to your infrastructure
- Traditional antivirus software only protects the endpoint

Prevention #1: Advanced Endpoint Detection

- Provides layered defenses - protects the many devices that connect the network
- Protects endpoints and the network together as part of a single ecosystem
- Protects by using machine-learning or behavioral analysis



Advantages #1: Advanced Endpoint Detection

- Can define a range of policies that minimize risks to all endpoints
- Can be deployed to remote endpoints- even if those are personal computers
- Ensures that everyone is working securely no matter where they are



Risk #2: Bring Your Own Headache

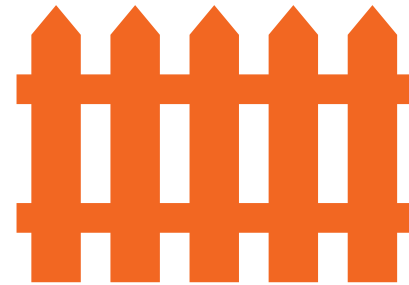


Source: Cisco 2020 Benchmark Report

- Wide scale use of public cloud services – Dropbox, Google Drive, iCloud, Zoom
- Workforces become more distributed, increased access to inappropriate websites or content

Prevention #2: Web Gateway Security

- Blocks access to websites or content based on acceptable use policies
- Enforces their security policies to make internet access safer
- Helps protect data against unauthorized transfer



Advantages #2 - Web Gateway Security

- Total peace of mind that all internet traffic is secure
- Centralized /consistent policies across all remote locations
- Better performance and user satisfaction



Risk #3: Your Pa\$\$word



CyberCriminals

- Purchase credentials, test for matches on other systems
- Use user lists, attempt the same password over a very large number of usernames

Prevention #3: Dark Web Research

- Understand if there are activities being plotted against your business
- Continuous monitoring for activity containing your business accounts
- Immediate identification of all business accounts stolen and/or for sale

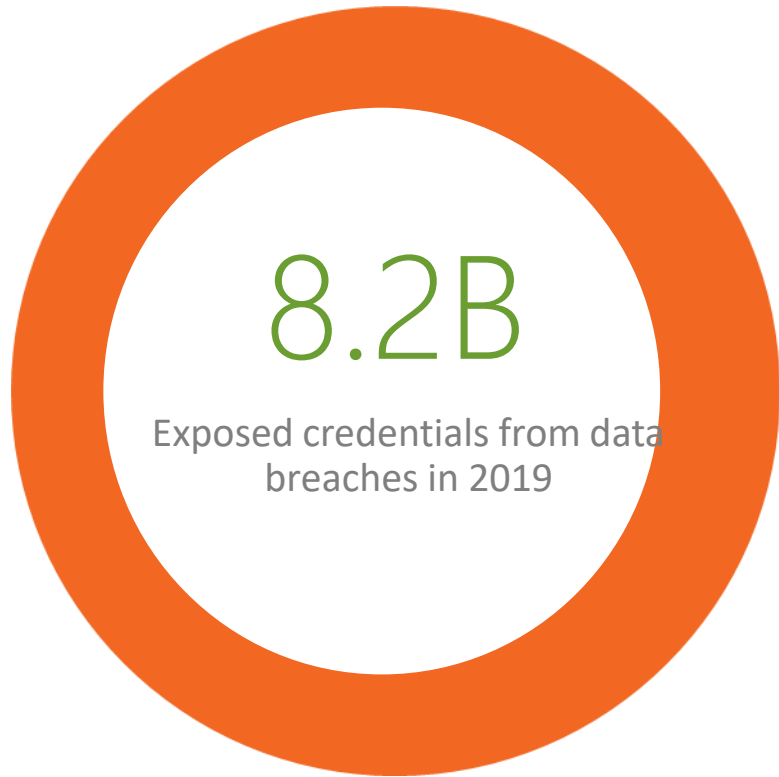


Advantages #3: Dark Web Research

- Reduced risk of account takeover, business email compromise and live hack
- Improved password policy awareness for both business and personal safety
- Improved awareness of threat actors and dark web activity



Risk #4: Leaving the Key Under the Doormat



- “username and password” approach to account security can be easily breached
- Employees do fall for phishing scams
- Biggest security threat today is the risk of compromised credentials

Prevention #4: Multi-Factor Authentication

- A process where a user is prompted during sign-in for an additional form of identification
- Ensures that even if your password does get stolen, your data stays protected



Advantages #4: Multi-Factor Authentication

- Keeps your business ahead of ever-changing security threats
- Verify identity in seconds
- Avoid an expensive data breach



- 10/ 7 - Being Prepared for an Incident

6 Ways to Protect Your Business From a Cyber Attack!

 <p>Security Assessment It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?</p>	 <p>Security Awareness Train your users- often! Teach them about data security, email attacks, and your policies and procedures.</p>	 <p>Spam Email Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks.</p>
 <p>Passwords Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, or set user screen timeouts.</p>	 <p>Computer Updates Keep Microsoft products updated for better security. Look for a "critical update" service via automation to protect from attacks.</p>	 <p>Log Management SEIM, Security Incident & Event Management uses big data engines to review all event and security logs from all covered devices.</p>
 <p>Firewall Turn on intrusion detection and intrusion prevention features. Send the log files to a managed SIEM.</p>	 <p>Encryption Whenever possible, the goal is to encrypt files at rest, in motion, and especially on laptops.</p>	 <p>Advanced Endpoint Detection Protects your computers data from malware, viruses, and cyber attacks through file-less and script-based threats.</p>
 <p>Multi-Factor Authentication Adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.</p>	 <p>Web Gateway Security Internet security is a race against time. Cloud based security detects web and email threats as they emerge and blocks them on your network within seconds.</p>	 <p>Dark Web Research Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach.</p>
 <p>Security Eng work with IT professions the framework for a security requ</p>	 <p></p>	 <p>Response Plan</p>

Cyber In

Thank you!

Justin Krentz:

Jkrentz@verticalsol.com

724-493-0933

Tyler Lewan:

tlewan@verticalsol.com

847-987-9606



Vertical  **Solutions**
an R.L. Nelson & Associates Company