Cybersecurity Training / Ransomware Legislation

State Representative
Giovanni Capriglione

Higher Priority for the Legislature

- Increasing privacy/breach concerns by constituents
- Increased Focus on Cybersecurity in Texas Agencies
- Increased Budget for Cybersecurity Programs and Assessments
- Increased Budget for legacy modernization

Recent Attacks in Texas

- May 10 2020
  - All Texas courts' websites were taken offline by the attack, including the website of the Texas Supreme Court, which was forced to issue opinions through Dropbox on Friday.
- May 14 2020
  - The Texas Department of Transportation determined that on May 14, 2020, there was unauthorized access to the agency's network in a ransomware event. TxDOT immediately took steps to isolate the incident and shut down further unauthorized access.
- August 20 2019
  - Computer systems in 22 Texas municipalities were infiltrated by hackers demanding a ransom. A mayor of one of those cities said the attackers asked for $2.5 million to unlock the files

HB 9

HB9 goes after the activity, not the technology, a more lasting approach to addressing cybercrime.

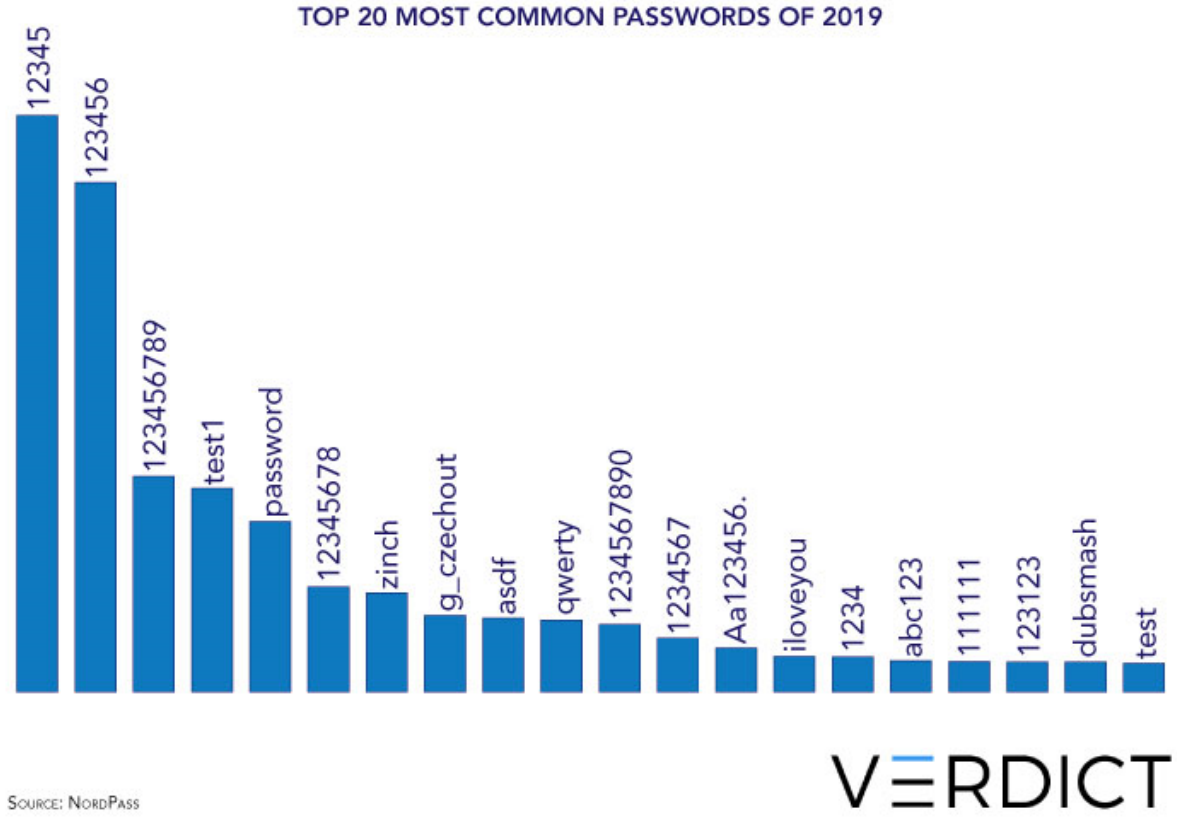
H.B. 9 creates an offense for intentionally interrupting or suspending access to a computer system or network without the effective consent of the owner.

Offenses and definitions for: DOS attacks, malware, ransomware, altering data and unlawful decryption.

Cyber Security Training

- The Problem: Even some of the strongest security systems may be bypassed or compromised by employees.
  - 94% of malware is distributed through email
  - Social Engineering / Phishing attacks make up 80%+ of reported incidents
  - Majority of successful attacks may have been prevented by updating with then available patches.
  - Dark Alleys
- NIST: "Your employees are your first line of defense against cyber attacks."

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%



35% of computer users never change their passwords.

Legislative Strategies

- Idea
- Stakeholders
  - Most likely to oppose
  - Ancillary Benefits
- Addressing Concerns
  - Vendor issues
  - Local Control
  - Fiscal note
- Member buy-in
- Rulemaking

HB 3834

- House Bill (HB) 3834 (86R) requires DIR to certify cybersecurity training programs and requires government employees /contractors to complete a certified training program.
  - Employees who have access to computer, contractors who have access to computers.

- Employee Training IS effective … if done correctly.
  - Focus on forming information security habits and procedures that protect information resources
  - Teach best practices for detecting, assessing, reporting, and addressing information security threats.

Training Programs

- To date over 100 certified programs
- Many are low cost or even free, some as short as 30 minutes long.
- Tailored for each employee / entity.
- To date: 34 state agencies have completed the training & 630 local government entities

Center for Information Security Awareness - CFISA
Security Awareness Training Lessons - 2020

Lesson 1: Course Introduction and Overview - 4:59 min

Cybercrime is the fastest growing crime in the world. Our personal and business accounts are being attacked daily. This lesson explains the importance of this course and provides an overview of the risk associated to cybercrime.

Lesson 2: The Impact of Cybercrime and Identity Fraud – 8:00 min

Cybercrime and identity theft are risk to the business and your personal information every day. Understanding the risk of computer malware and how to protect your business and personal information is important to everyone.

Lesson 3: Today's Threats – 7:39 min

There are many different types of cyber threats included in cybercrime, but most fall into one of just five categories. Understanding these threats and ways to protect against these crimes are covered in this lesson.

Lesson 4: How Behavior is Exploited by Cybercriminals – 9:27 min

Hackers do their homework studying the predictable behavior of employees like you. Criminals try to find vulnerabilities they can exploit to attack your workplace. Social engineering methods and day to day security practices are discussed in this lesson.

Lesson 5: Strong Passwords Increase Security – 9:36 min

Your password is key to your online security at work and at home. Learn how passwords can easily be exploited and what you can do to maximize the security of your password.

Lesson 6: Understanding and Recognizing Social Engineering – 4:26 min

One of the most effective and dangerous techniques hackers use to manipulate employees is called social engineering, and it's critically important that you learn how to recognize this serious threat.

Lesson 7: Phishing and Email Best Practices – 6:35 min

Phishing email attacks are the number one risk to our business and personal email accounts. Learning email best practices will reduce the risk for everyone. How to safely handle email and recognizing phishing scams is key to day to day security.

Lesson 8: Protecting Against Viruses, Spyware and Spam – 6:30 min

Your workplace is a target for computer viruses, spyware, keyloggers and other malicious code that are designed to steal confidential information. Learning how to recognize these threats will greatly reduce your risk.

Lesson 9: Protecting Your Personal Workspace – 11:09 min

Protecting your physical workspace is an important part of day to day security and is directly connected to information security risk. Knowing how to protect your personal workspace will make your overall physical security better. NIST - Guidelines for Media Sanitization is covered in this lesson.

Lesson 10: Security Best Practices Away from the Office – 9:37 min

Security doesn't end when you leave your workplace. Learn how to protect your data when away from the office. Laptop and device protection, telecommuting security, and working securely on the road are all covered in this lesson.

Lesson 11: Safe Internet Use – 6:09 min

Understanding the risk associated to using the Internet will help to protect your business and personal data. Workplace policies and procedures involving safe Internet use are discussed in this lesson.

Lesson 12: Protecting the Workplace from Identity Fraud – 6:58 min

Identity theft is one of the fastest growing crimes. Prevention of this crime can begin in the workplace. Learn how to protect yourself, your family, and your workplace through better awareness.

Lesson 13: Social Media Security – 11:02 min

The risk associated to using social media sites are important to our work and personal security. Day to day risk associated to using social media along with ways to protect our social media accounts will be covered in this lesson.

Lesson 14: Device Management – Internet of Things – 7:25 min

We now have many devices and applications connecting to the Internet, all with different security settings. Understanding all the ways we connect to the Internet of things is necessary to protect our safety and security.

Lesson 15: Todays Risks - Acceptable Use of Electronic Resources – 7:46 min

The protection of information handled by computer networks is a key part of a security strategy. This lesson provides an explanation of workplace policy guidelines on safe and acceptable use of electronic resources.

***Lesson PCI-DSS Overview - 5:55 min (PCI Level I & II Courses ONLY)**

PCI-DSS compliance and secure handling of credit card data is important to the safety, security and success of the business. This lesson provides an overview of PCI-DSS compliance including why the policies and procedures are required and how you can help.

Additional Resources and Sources

- https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
- https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-starts-your-employees
- https://nordpass.com/blog/top-worst-passwords-2019/
- https://www.pcmag.com/news/35-percent-of-people-never-change-their-passwords
- https://www.theguardian.com/money/blog/2012/sep/28/debit-cards-currentaccounts
- https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154#cybersecurity
- Training source: https://www.cfisa.com/