

CSIS LIST OF SIGNIFICANT CYBER INCIDENTS

January 2019 - **August 2019**, Networks at several Federal government agencies and critical infrastructure providers were infiltrated by hackers linked to Iran.

January 2019 - **August 2019**, A previously unidentified Chinese espionage group was found to have worked since 2012 to gather data from foreign firms in industries identified as strategic priorities by the Chinese government, including telecommunications, healthcare, semiconductor manufacturing, and machine learning. The group was also active in the theft of virtual currencies and the monitoring of dissidents in Hong Kong.

January 2019 - **August 2019**, Russian hackers were observed using vulnerable IoT devices like a printer, Wi-Fi phone, and video decoder to break into high value corporate networks.

January 2019 - **August 2019**, A seven-year campaign by an unidentified Spanish language espionage group went.

January 2019 - **August 2019**, It was revealed to have resulted in the theft of sensitive mapping files from senior officials in the Venezuelan Army.

January 2019 - **August 2019**, State-sponsored Chinese hackers conducted a spear phishing campaign against employees of three major U.S. utility companies.

January 2019 - **August 2019**, The U.S. Department of Justice announced an update to its guidance on how to best protect corporate data.

January 2019 - **August 2019**, The U.S. Department of Justice announced an update to its guidance on how to best protect corporate data.

January 2019 - **August 2019**, A previously unidentified Chinese espionage group was found to have worked since 2012 to gather data from foreign firms in industries identified as strategic priorities by the Chinese government, including telecommunications, healthcare, semiconductor manufacturing, and machine learning. The group was also active in the theft of virtual currencies and the monitoring of dissidents in Hong Kong.

January 2019 - **August 2019**, Russian hackers were observed using vulnerable IoT devices like a printer, Wi-Fi phone, and video decoder to break into high value corporate networks.

January 2019 - **August 2019**, A seven-year campaign by an unidentified Spanish language espionage group went.

January 2019 - **August 2019**, It was revealed to have resulted in the theft of sensitive mapping files from senior officials in the Venezuelan Army.

January 2019 - **August 2019**, State-sponsored Chinese hackers conducted a spear phishing campaign against employees of three major U.S. utility companies.

January 2019 - **August 2019**, The U.S. Department of Justice announced an update to its guidance on how to best protect corporate data.

January 2019 - **August 2019**, The U.S. Department of Justice announced an update to its guidance on how to best protect corporate data.

RANSOMWARE ATTACK HITS 22 COMMUNITIES IN TEXAS – AUGUST 16, 2019

Multiple entities in Texas reported a ransomware attack. Entities included governmental agencies and at least one critical infrastructure SCADA system and two military bases.

Region 1 – Collin County: City of Lavon Police Department, Dallas County: City of Cockrell Hill PD, City of Wilmer; Ellis County: City of Palmer; Kaufman County: City of Kaufman PD; Johnson County: City of Keene; City of Venus Police Department; Hopkins County: Sulphur Springs Police Department; Lamar County: Lamar County Sheriff's Office; City of Reno Police Department; Cooke County: Gainesville PD; Fannin County: Bonham PD; Grayson County: Grayson County Sheriff's Office.

Region 2 – Robertson County: Robertson County Sheriff's Office.

Region 3 – Situation: None reported.

Region 4 – San Angelo: Reagan County Sheriff's Office.

Region 5 – Lubbock County: EMC; Terry County: Terry County Sheriff's Office, Yoakum County: City of Plains; Wilbarger County: Vernon PD; Young County: Graham PD.

Region 6 – Situation: Bastrop County: Elgin PD; Bexar County: Randolph AFB Security Forces and Fort Sam Houston AFB Security Forces; Lampasas County: City of Lampasas PD.

Region 1 – Collin County: City of Lavon Police Department, Dallas County: City of Cockrell Hill PD, City of Wilmer; Ellis County: City of Palmer; Kaufman County: City of Kaufman PD; Johnson County: City of Keene; City of Venus Police Department; Hopkins County: Sulphur Springs Police Department; Lamar County: Lamar County Sheriff's Office; City of Reno Police Department; Cooke County: Gainesville PD; Fannin County: Bonham PD; Grayson County: Grayson County Sheriff's Office.

Region 2 – Robertson County: Robertson County Sheriff's Office.

Region 3 – Situation: None reported.

Region 4 – San Angelo: Reagan County Sheriff's Office.

Region 5 – Lubbock County: EMC; Terry County: Terry County Sheriff's Office, Yoakum County: City of Plains; Wilbarger County: Vernon PD; Young County: Graham PD.

Region 6 – Situation: Bastrop County: Elgin PD; Bexar County: Randolph AFB Security Forces and Fort Sam Houston AFB Security Forces; Lampasas County: City of Lampasas PD.

NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Cyber-Risk Oversight Handbook's five key principles:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue
2. Directors should understand the legal implications of cyber risk as they relate to their company's specific circumstances
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas

NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Cyber-Risk Oversight Handbook's five key principles:

4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget
5. Board-management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach

TML TEXAS MUNICIPAL LEADER

CYBER WARRIOR

ORGANIZATION STRUCTURE REFLECTS EMPHASIS

TML TEXAS MUNICIPAL LEADER

CYBER WARRIOR

STARTS AT THE TOP

Choose the right Cyber Champion

Stay Anchored to a Meaningful Mission

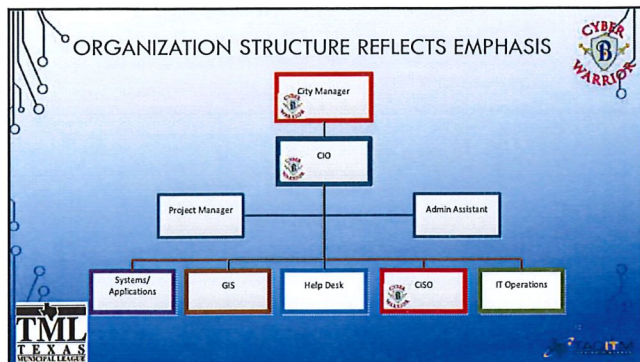
City Council, Direct Reports, Senior Staff
Awareness, Culture, Training

Front Line Managers & Supervisors
Motivational, Awareness, Phishing, Social Engineering & Response Training

Employees
Motivational, Awareness, Phishing, Social Engineering & Response Training

TML TEXAS MUNICIPAL LEADER

CYBER WARRIOR



CYBER CHAMPION ROLE

- ✓ Cyber Champion MUST recognize and address both technical concerns and end-user's "digital rhythm"
- ✓ Recognize throwing money at technology does not keep attackers out or breaches from happening
- ✓ Speak to real-life issues at all levels of the organization and community
- ✓ Once interaction with data (**digital rhythm**) is understood, develop and use training to mitigate cybersecurity risks before damage can be done

The slide features a cartoon of a boxer in a ring, with a speech bubble that reads: "IN THIS CORNER WE HAVE SKILLFUL, DEDICATION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!". The slide also includes logos for TML Texas Municipal League and Cyber Warrior.

HOW?

1. Empower USERS by creating a culture of cybersecurity awareness
2. Ensure USERS understand the value of the Information USERS interact with on a daily basis
3. Give USERS the knowledge and tools to be THE first line of defense
4. A Security Awareness Program is designed to arm USERS with the tools and practical knowledge to understand and identify common security threats to make the correct quick decisions when it comes to protecting information and assets
5. Consistent and constant messaging

The slide lists five ways to implement a security awareness program. It includes icons for Password, Network, Security, Cyber Change, Security Awareness, and Communication. The slide also includes logos for TML Texas Municipal League and Cyber Warrior.

TRAIN USERS TO BE CYBER-SMART
HOME, WORK & TRAVEL



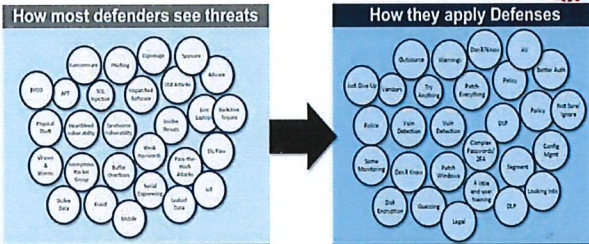
Home Work Public WiFi

By changing YOUR DIGITAL RHYTHM EVERYWHERE




The "Normal" IT Defenders Approach to Threats

Poor risk analysis leads to mis-ranked, whack-a-mole, defenses




How most defenders see threats

How they apply Defenses

"Like bubbles in a glass of champagne"

"Every defense is treated equally, or applied disproportionate to risk"

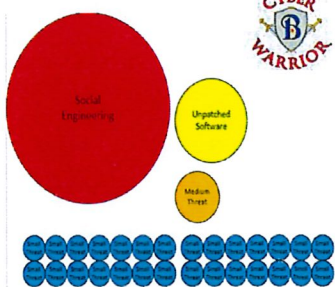



Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software

Preventative Controls

- Technical
- Training





EMAIL VOLUME

We get A LOT of emails!

We cannot stop everything

Month-Year	Total Inbound Email	Rejections (Includes Virus & Spam)	Legit Inbound Email	% Rejections	Total Outbound Email	Total Internal Email
Aug - 2018	232,248	83,145	149,103	35.8 %	113,729	15,316
Sep - 2018	217,670	81,207	136,463	37.32 %	78,628	15,907
Oct - 2018	265,870	113,064	152,806	42.53 %	93,156	22,859
Nov - 2018	269,660	119,033	140,627	45.84 %	80,806	17,501
Dec - 2018	274,464	145,642	128,822	53.06 %	67,976	14,696
Jan - 2019	331,135	179,330	151,805	54.16 %	89,102	18,644
Feb - 2019	281,632	147,018	139,614	50.43 %	80,920	16,391
Mar - 2019	305,420	159,915	145,505	52.36 %	76,829	16,157
Apr - 2019	276,219	126,031	150,188	45.63 %	87,115	15,162
May - 2019	278,277	128,739	149,539	46.26 %	103,831	17,005
June - 2019	249,610	113,268	135,342	45.56 %	93,644	15,304
July - 2019	271,827	136,342	135,485	50.16 %	120,658	18,353
Total	3,242,932	1,527,733	1,715,199		1,086,394	201,295
Mean	279,244.34	127,311.09	142,933.25	45.59 %	99,532.84	16,774.58

PHISHING CAMPAIGN AND "RULES OF ENGAGEMENT"

1. Monthly Phishing Campaigns, occasionally more, be ready - At least one Phishing email per campaign (could be more...)
2. Failing a simulated phishing email campaign – "Clicking"
3. Clickers - both user and manager are notified of the failed phishing campaign
4. User auto enrollment into progressive training

PHISHING CAMPAIGN AND "RULES OF ENGAGEMENT"

- All Clickers have 2 weeks to complete assigned training
- Not taking or passing the required training within 2 weeks
 - User, Manager, and CIO are notified network access is disabled until scheduled through Helpdesk to complete the training at the IT building during normal business hours


PHISH ALERT BUTTON (PAB) AND SECOND CHANCE

PAB

- Report suspicious emails
- Pro-active role in controlling the volume of malicious emails
- Provides IT with early warning
- Helps YOU become interactive with YOUR Cybersecurity awareness
- Receive instant feedback for reporting the email, thanking YOU for keeping the COB secure

Second Chance

- Second Chance Alert empowers YOU to make smarter security decisions by providing YOU a "second chance" to back out of a click

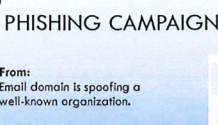


PHISHING CAMPAIGNS

From:
Email domain is spoofing a well-known organization.


Breaking News
Shocking Content to entice you to click link or open attachment.

Links:
Hover over the link. Link is taking you to a different address then what is shown.



BREAKING NEWS:
Nancy Pelosi to Announce Stepping Down as Speaker of the House

With mounting pressure from both the left and right wings of the Democratic Party, Rep. Nancy Pelosi announced she will be stepping down as Speaker of the House, effective April 1, 2019. [Click here](#) to watch the full video.



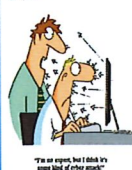
Read more about Pelosi's resignation at ABC News.

This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It may contain information that is exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy regarding FOUO information. Do not release this information to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. Do not copy, retransmit, disseminate, or otherwise use this information for purposes not intended by the sender. If you are not an intended recipient, please do not print, copy, retransmit, or otherwise use this information. If you are not an intended recipient, please do not print, copy, retransmit, or otherwise use this information. If you are not an intended recipient, please do not print, copy, retransmit, or otherwise use this information.

City of Bryan 20 Month PPP

Month	Percent under Poverty line
Jan 2017	11.3
Feb 2017	11.8
Mar 2017	3.8
Apr 2017	4.8
May 2017	3.8
Jun 2017	3.5
Jul 2017	3.5
Aug 2017	4.8
Sep 2017	4.6
Oct 2017	3.8
Nov 2017	3.3
Dec 2017	3.8
Jan 2018	3.2
Feb 2018	3.8
Mar 2018	3.8
Apr 2018	3.8
May 2018	3.8
Jun 2018	3.8
Jul 2018	0.25
Aug 2018	0.6
Sep 2018	0.7


FROM FRONT PERCENTAGE												
Year	Month	Conth	FD con	RTU con	Riv con	ConZee	ITW	Pub/Wh/LSU	ConGWS	FD conZee	Spd con	Standard Deviation
2014	Nov	2.91	2.7	2.8	2.3	0	2.6	5.1	2.9	0	3.1	1.98
2015	Nov	2.34	3.2	1.4	2.3	0	0	3	0	0	3.6	1.66
2016	Dec	2.85	3.1	0.6	4.3	2.6	5	3.5	1.3	0	0	1.76
2017	Feb	1.79	2.1	0.7	1.6	3.9	0	1.1	0.7	0	0.3	1.51
2018	Feb	2.26	2.7	2	3.8	2.5	0	2.9	0	0	1.8	1.53
2019	Mar	1.19	0.5	1.3	2.1	2.7	0	1.3	0	0	1.7	1.00
2020	Apr	2.37	4.3	0.8	1.4	1.1	0	3.4	1.9	0.3	1.7	3.76
2021	Jun	2.81	3.5	0.9	2.1	0	0	3.1	5.1	0.4	1.9	4.42
2022	Jul	0.33	0.15	0	0	0	0	1.03	0	0	0.36	0.43
2023	Aug	0.62	0.5	0.1	0	0	0	1.5	0	0	1.8	0.75
2024	Dec	0.7	1.6	0.5	0.7	0	0	0.03	0	0	0	0.13
Current Run May												
6/5/24	1.90	2.39	1.97	2.63	2.50	0.56	2.55	1.71	4.42	1.42	1.20	2.23
* Average Results												
2014	2	1	2	1	1	1	1	1	3	3	9	1





It's an expense, but I think it's worth it.

CHANGING OUR "RHYTHM"

CITY OF BRYAN PERFORMANCE EVALUATION FORM (For Non-Supervisory Employees)




14	Training	Successfully completes the training requirements set forth in the Training and Talent Development Program for the review period. Ensures the 2 Year required training course requirements are met. Tracks and submits a log of all training courses, internal and external training included.	<input type="checkbox"/> Meets <input type="checkbox"/> Does Not Meet
15	Cyber Security	Consistently displays awareness and aptitude of cybersecurity threats/attacks, fraudulent activity potential, and social engineering tactics in the context of information security. Understands the impact and negative effects a successful cyber-attack or social engineering scheme can have on the City of Bryan's public image, reputation, and financial position.	<input type="checkbox"/> Meets <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Not Applicable






CYBER SECURITY AWARENESS TRAINING POLICY

REMEDIAL ACTION FOR CYBER SECURITY DEFICIENCIES




By design, the internal phishing campaign emails mimic real world phishing attempts. Employees with high "click rates" and higher Phish Prone percentages tend to suggest a general lack of understanding and/or willingness to comply with the Cyber Security Awareness Program. **As a result, these actions place the City and its network at an elevated cyber risk.** In certain instances, the City will use a progressive disciplinary system. The City is not obligated to use all of the progressive disciplinary steps available to it, and may begin the disciplinary process at any level, up to and including immediate termination, depending on the severity of the conduct, the employee's work performance and prior disciplinary history, the employee's length of service, and any mitigating circumstances.



CYBER SECURITY AWARENESS TRAINING POLICY

REMEDIAL ACTION FOR CYBER SECURITY DEFICIENCIES



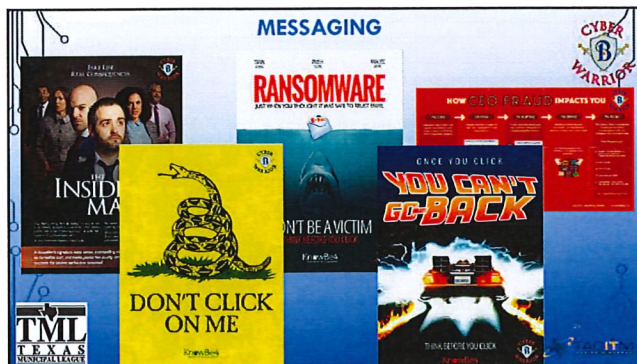
Depending on the circumstances of each individual case, disciplinary action may consist of one or more of the following: **1) Oral warning; 2) Letter of counseling; 3) Written reprimand; 4) Probation; 5) Suspension without pay; 6) Demotion; 7) Termination**

The following table provides guidelines and an example of how disciplinary action might be imposed due to non-compliance and/or unwillingness to adhere to this policy in a **12-month period**. It is intended as a process designed for self-improvement by the employee and supervisor/manager but may result in punitive action. Managers may use discretion within the parameters of the table, or outside the parameters, if appropriate and coordinated with Human Resources, based on circumstances of the situation.

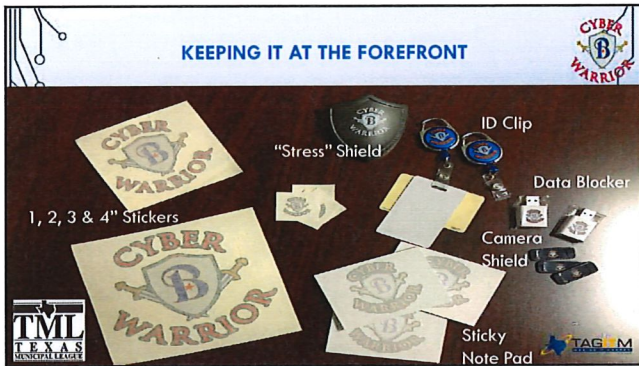



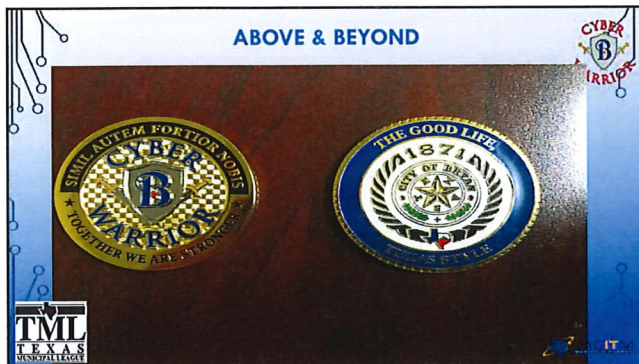
"Click" Count	Resulting Level of Remedial Action
First Failure	Mandatory completion of selected course(s) by the Information Technology (IT) Department
REMEDIAL ACTION FOR CYBER SECURITY DEFICIENCIES	<ul style="list-style-type: none"> - Discussion with Supervisor/Manager on the importance of Cyber Security Awareness - Appropriate level of discipline, if applicable, working with Human Resources (HR)
Second Failure	Mandatory completion of selected course(s) by the IT Department <ul style="list-style-type: none"> - Notice to the appropriate Executive Director (ED) - Appropriate level of discipline, if applicable, working with HR - A Performance Improvement Plan (PIP) may be initiated - "Does Not Meet" expectations in the Cyber Security Awareness category in the appropriate annual performance review period
Third Failure	Mandatory completion of selected course(s) by the IT Department <ul style="list-style-type: none"> - Notice to the appropriate ED - Appropriate level of discipline, if applicable, working with HR - Initiate PIP or follow up or addition to existing PIP

"Click" Count	Resulting Level of Remedial Action
Fourth Failure	Mandatory completion of selected course(s) by the IT Department <ul style="list-style-type: none"> - Notice to the appropriate ED - Appropriate level of discipline, working with HR - Follow up or addition to PIP (depending on timeframe and language of original PIP) - Discuss or review transfer options to a position not requiring cybersecurity proficiency and awareness (if a position is available) - Administrative and technical control options discussed and/or implemented
Fifth Failure	Mandatory completion of selected course(s) by the IT Department <ul style="list-style-type: none"> - Formal review of employment with the Human Resources Director and ED - Appropriate level of discipline, working with HR - Discuss or review transfer options to a position not requiring cybersecurity proficiency and awareness (if a position is available) - Restricted network access may be implemented
Sixth Failure	Formal review of employment with the Human Resources Director and appropriate Executive Director and City Manager <ul style="list-style-type: none"> - Disconnection from the City network may be implemented










QUESTIONS?

Any Questions for us? Just email:
Bernie Acre, CIO: bacre@bryantx.gov
Scott Smith, CISO: ssmith@bryantx.gov



TML TEXAS MUNICIPAL LEADER

CYBER WARRIOR

RESOURCES

Center for Information Security (CIS) <https://www.cisecurity.org/>
 CIS 20 Critical Controls: <https://www.cisecurity.org/controls/>
 Benchmarks: Secure Configurations for 140+ Operating Systems and software
 Hardened Images: <https://www.cisecurity.org/hardened-images/>
 CIS SecureSite: <https://www.cisecurity.org/cis-secure-site/> (Free Membership)
 Free Tools and Resources
 CIS-CAT Pro – Vulnerability & Benchmark scanning tool
 MS-ISAC: <https://www.cisecurity.org/ms-isac/> (Free Membership)
 24/7 Security Operation Center
 Incident Response Services
 Cybersecurity Advisories and Notifications
 Access to Secure Portals for Communication and Document Sharing
 Cyber Alert Map
 Malicious Code Analysis Platform (MCAP)
 Weekly Top Malicious Domains/IP Report
 Monthly Members-only Webcasts
 Access to Cybersecurity Table-top Exercises
 Vulnerability Management Program
 Nationwide Cyber Security Review (NCSR)
 Awareness and Education Materials

TML TEXAS MUNICIPAL LEADER

CYBER WARRIOR

RESOURCES

DHS Free Services: https://www.us-cert.gov/its/default.aspx?cid=3&ip=it/UIT_Hands_On_Support.pdf

- Cybersecurity Assessments
- Cyber Resilience Review
- External Dependencies Management Assessment
- Cyber Infrastructure Survey
- Phishing Campaign Assessment
- Risk and Vulnerability Assessment
- Vulnerability Scanning
- Validated Architecture Design Review (VADR)
- Cybersecurity Evaluation Tool (CSET)
- Cybersecurity Resources and Awareness
- Information Products: National Cyber Awareness System
- STORThink, COH-ICE
- National Initiative for Cybersecurity Careers and Studies
- Federal Virtual Training Environment (FedVTE)
- Cybersecurity Consulting
- Cybersecurity Advisors
- Cybersecurity Exercises
- Information Sharing and Threat Analysis
- Homeland Security Information Network (HSIN)
- Automated Indicator Sharing
- Malware Analysis
- Cyber and Communications Incident Response
- Malware Traffic, Analysis, and Cyber Threat Hunting Threat Bank
- National Cybersecurity Center for Communications Watch
- National Trust Center
- Continuous Operations and Migration Program

TML TEXAS MUNICIPAL LEADER

CYBER WARRIOR

RESOURCES

NIST Cybersecurity Framework: <https://www.nist.gov/cyberframework>
 Risk Based
 Flexible
 Profiles – Measure improvement over time
Idaho National Labs – Free ICS Training
<https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT>
 Need to pay your way there

Resources –
 AuditScripts: <https://www.auditscripts.com/free-resources/critical-security-controls/> – This is a free assessment tool to help evaluate the implementation of the CIS 20 Critical Controls
 Platform for awareness training combined with simulated phishing attacks – www.knowbe4.com
 The Human Nature of Cybersecurity – <https://es.siftsworld.com/articles/2019/5/the-human-nature-of-cybersecurity/#p12>
 Platform for training and email filtering – <https://www.siftsworld.com/cybersecurity/>
 The Human Nature of Cybersecurity – By understanding cognitive biases and shortcuts, we can better engage people to improve cybersecurity awareness, behavior, and culture.
 Research Summary: <https://www.siftsworld.com/articles/2019/5/the-human-nature-of-cybersecurity/#p12>

TML TEXAS
 TARRANT COUNTY
 TARRANT COUNTY

CYBER WARRIOR

RESOURCES

National Association of Corporate Directors (NACD) Cyber-Risk Oversight – Directors Handbook Series
<https://www.nacdonline.org/enlight/publications/cyberitemNumber=10687>
Norton ISTR (Internet Security Threat Report, Volume 24, February 2019 – <https://www.symantec.com/security-center/threat-report>
Ponemon Institute and IBM – 2016 Cost of Data Breach Study: Global Analysis, p. 2.
<https://www.ibm.com/security/data-breach>
Timar Kessem – “2016 Cybercrime Reloaded: Our Predictions for the Year Ahead,” Jan. 15, 2016
<https://www.securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead/>
Verizon – 2016 Data Breach Investigations Report, p. 8–9 <https://enterprise.verizon.com/resources/reports/dbr/>
Kessem – “2016 Cybercrime Reloaded”
<https://www.securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead/>
FireEye Inc – Mandiant M-Trends 2016, p. 4
https://www.fireeye.com/content/dam/ftt/2016/M-Trends-2016-1P_Mandiant.pdf
Jeff Goldman – “48 Percent of Companies Don’t Inspect the Cloud for Malware,” eSecurity Planet, Oct. 12, 2016
<https://www.esecurityplanet.com/news/48-percent-of-companies-dont-inspect-the-cloud-for-malware/>
Thy Olayarad – “Companies complacent about data breach preparedness,” CIO, Oct. 28, 2016
<https://www.cio.com/article/3535871/companies-complacent-about-data-breach-preparedness>

TML TEXAS
 TARRANT COUNTY
 TARRANT COUNTY

CYBER WARRIOR

RESOURCES

SANS Security Awareness Tip of The Day - <https://www.sans.org/tip-of-the-day>
Digital Attack Map - www.digitalattackmap.com
Texas Cyber Attacks - <https://www.secure.com/cyber-attacks-texas>
MITRE ATT&CK - <https://attack.mitre.org/>
CSIS (Center for Strategic & International Studies) - <https://www.csis.org>
DHS Stop.Think.Connect.™ Public Awareness Campaign - www.dhs.gov/stopthinkconnect

TML TEXAS
 TARRANT COUNTY
 TARRANT COUNTY

CYBER WARRIOR
