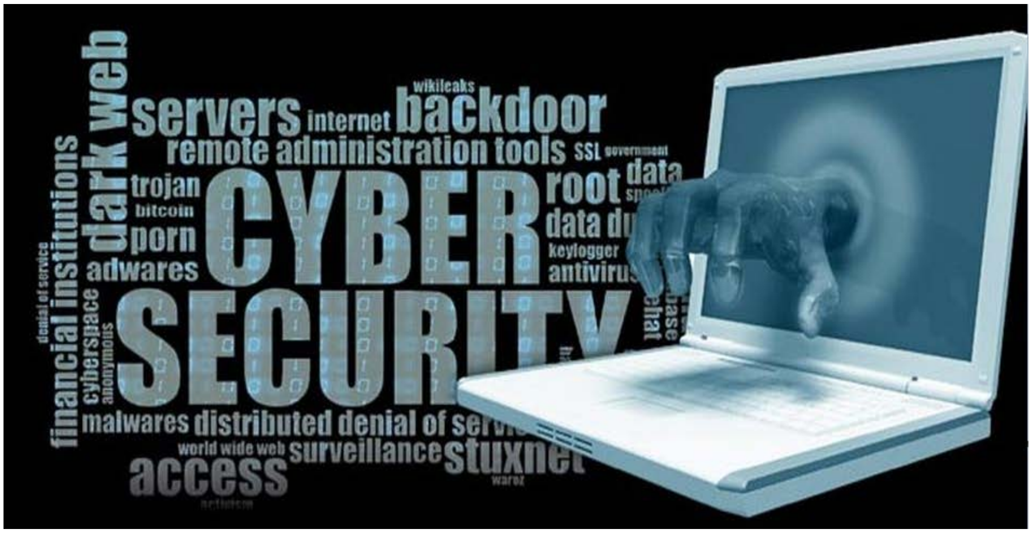

Security Awareness / Trends

January '18

2018 THREATS

Cybersecurity Predictions in 2018

What We Learned

In 2017 we saw some of the previous security threats continue to top the list. Ransomware, Phishing and Internet of Things attacks were still highly successful and the ability to find these attacks being sold as a service only added to their increased occurrence. Security professionals stated that the primary protection from these attacks as being security awareness training, cybersecurity insurance and data access governance programs. As an institution we have aligned well with these recommendations. We are improving our annual training to include topics covering phishing and data classification. We have cybersecurity insurance in place in the event of an incident and protect data access through a least privilege approach and formal access request process.

What to Expect

Looking ahead to 2018 here is a brief list of 10 predictions from *eWeek*.

1. **Africa emerges as new area of cyber threats.** We have already seen this at JCCC with the last round of phishing that originated from Nigeria.
2. **AI vs AI.** Cyber-attacks are using artificial intelligence (AI) based attacks to mimic human behavior in an effort to avoid detection.
3. **GDPR Means Good Enough Isn't Good Enough.** General Data Protection Regulation (GDPR) which goes into effect this year may have impact on colleges and universities. If an institution receives admissions forms from EU residents there are regulations that may need to be applied while processing this data.
4. **Consumerization of Cybersecurity.** This may be in large part to the Equifax data breach. In the coming year consumers will have options to purchase not only antivirus protection but packages that would include identity and credit monitoring.
5. **Ransomware Will Continue.** WannaCry and NoPetya made the headlines in 2017 and there is no reason to think that another threat is not looming in 2018.
6. **Denial of Service Will Become Financially Lucrative.** A botnet of Internet of Things devices brought the Internet to a crawl but now attackers are looking to monetize this ability against organizations that are dependent on cloud services and online presence.
7. **Health Care Will be a Favored Target.** Health care have large amounts of Personally Identifiable Information (PII) and have increased value on the black market. Targeting medical devices that are not easily updated and less secure puts this data at high risk.
8. **The Year of MFA.** Multifactor Authentication will be implemented across more applications. As credentials are and identities become the defensible perimeter putting additional protections in place will be necessary.
9. **Cryptocurrencies Become the New Playground for Identity Thieves.** Bitcoin has been a big buzz with its rise in value. The rise in value will result in legislation to focus on trader identity.
10. **Automation Will Improve the IT Skills Gap.** There is continued adoption of new technology and the use of more advanced analytics. Automation with cloud services will be a big push in 2018.

Cybersecurity Trends Organizations Need to Brace for in 2018, http://www.eweek.com/security/18-cyber-security-trends-organizations-need-to-brace-for-in-2018 (accessed Jan. 2018)