SecurityFirst™
Data-Centric Cyber Solutions

THE CYBERSECURITY CHEAT SHEET

CYBERSECURITY 101

Election Security

Being able to ensure the integrity and security of state elections is crucial to maintaining the function of democracy in the United States and is a shared responsibility among government officials. Recently, state cybersecurity officials have been tasked with improving elections security. Additionally, legislators have set policy around elections security which can be cybersecurity or physical security. In early 2018, President Trump signed the Consolidated Appropriations Act of 2018 into law, which provided $380 million in the Help America Vote Act (HAVA). This act provides grants for states to make election security improvements.

If you want to learn more about election security and the current initiatives around this topic click on the links below:

- Election Security 101
- Election Security HAVA Funding by State

Malware Attacks

Malware is short for malicious software. It can be described as unwanted software that is installed on a device without consent. Viruses and worms are examples of malicious software and are among the most frequent forms of cyberattacks against individuals, although malware effecting businesses and government agencies has been known to occur. When malware takes effect, its goal is to damage, invade or disable computer systems, mobile devices and tablets. Additionally, it can steal, delete or encrypt data or spy on computer activity without knowledge or permission.

If you want to learn more about malware and how to prevent exposure click on the links below:

- What is Malware?
- List of Malware Types
- How to Avoid Malware

Phishing Attacks

Phishing attacks are focused on the weakest link in the security chain, human beings. Phishing is used to get access to computer networks and systems to deploy malware or gain unauthorized access to data. This is done most often through emails purporting to be from reputable companies in an attempt to persuade individuals to reveal personal information such as credit card numbers, passwords and other personal information.

Check out the links below for more about phishing and how to prevent exposure:

- What is Phishing?
- Ways to Prevent Phishing
- How to Avoid Exposure to Phishing

Data Privacy

Data Privacy is about the policies and procedures around the authorized access and use of personal data. Also known as information privacy, It is defined as only using collected data for the purpose it was intended, only for the time it is needed and only by users who's job function is to process the data as authorized by the ultimate owner, the data subject themselves. Currently, 48 states have passed laws requiring individuals to be notified if their information is compromised. The EU recently passed the general data protection regulation that provides protections for user data and privacy.

Click on the links below for more about Data Privacy and current initiatives:

- Guide to Protecting Personal Data
- More Information on GDPR

Data Security

Data security is the process of shielding data, computers and websites from unauthorized access and corruption. This can be done through data backups, authentication where users must provide a password, code or other form of data to verify identity before access is granted, or encryption which renders data unreadable to unauthorized users and attackers. Organizations around the globe are investing in defense capabilities to protect critical assets from access by unauthorized users who can find and sell personal user data.

For more resources about data security and how to prevent exposure click on the links below:

- Data Security Resources and Rules
- Starting with Data Security

SecurityFirst™
Data-Centric Cyber Solutions

THE CYBERSECURITY CHEAT SHEET

TOP AREAS OF LEGISLATIVE CYBERSECURITY ACTIVITY

Regulation Around Data Privacy

DATA SECURITY LAWS/PRIVATE SECTOR

Personal and identifying information is often collected by businesses and stored in various formats--digital and paper. Over 22 states currently have laws that require businesses that own, license or maintain personal information of an individual from that state, to maintain reasonable security procedures and practices.

For a full list of data security laws governing the private sector click on the link below:

- Full List of Data Security Laws/Private Sector

GENERAL DATA PROTECTION REGULATION

General Data Protection Regulation (GDPR) came into effect on May 25, 2018. It applies to organizations around the world that process or hold the personal data of individuals residing in the European Union. GDPR brings stronger protection of personal information and strong restrictions on how businesses and governments can store and monetize user data.

For more information on GDPR and what it means for consumers and businesses check out the links below:

- Will the EU's GDPR Rules Launch a New Era of Data Protection?
- GDPR Data Privacy Rights
- GDPR FAQs

CALIFORNIA CONSUMER PRIVACY ACT

The California Consumer Privacy Act was passed by the state of California legislature and signed by its governor on June 28, 2018, officially called AB -375. Beginning January 1, 2020, the bill will grant a consumer the right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer. In addition, the bill will grant a consumer the right to request deletion of personal information and the business to adhere to that consumers request.

For more information on the California Consumer Privacy Act, click on the links below:

- What You Need to Know About California's New Data Privacy Law
- California Consumer Privacy Act

GRAMM-LEACH-BLILEY ACT (GLBA)

Established in 1999, the Gramm-Leach-Bliley Act requires financial institutions, described as companies that offer consumers financial products or services like loans, financial or investment advice, or insurance, to explain their information sharing practices to customers and to safeguard sensitive data.

If you would like to learn more about the Gramm-Leach-Bliley Act, make sure to visit the links below:

- Gramm-Leach-Bliley Act
- Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information)

CANADA PRIVACY ACT (FEDERAL) AND PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

PIPEDA is a Canadian law relating to data privacy received Royal Assent on April 13, 2000 and came into force in stages beginning on January 1, 2001 and full into force on January 1, 2004. PIPEDA outlines how businesses are required to handle personal information. Organizations covered by PIPEDA must obtain and individual's consent when they collect, use or disclose that individual's information.

Click on the links below if you would like to learn more about PIPEDA:

- PIPEDA in Brief

Improving Government Security Practices

CYBERSECURITY LEGISLATION

According to the National Conference of State Legislatures, at least 35 states, D.C. and Puerto Rico have introduced or considered more than 265 bills or resolutions related to cybersecurity, improving government security practices being one of the goals.

For a full list of the legislation in place for 2018 check out the links below:.

- Cybersecurity Legislation 2018
- 8 Ways Governments Can Improve Their Cybersecurity

Providing Funding for Cybersecurity

FEDERAL FUNDING

The 2019 President's Budget increases allocations towards cybersecurity-related activities $583 million over 2018 levels. Over 70 federal agencies included cybersecurity funding in their 2019 budgets, since every agency is independently responsible for protecting its IT systems and data from cyber attack.

For more information on how funding is split between agencies and for the full budget click the links below:

- Cybersecurity Funding Allocations
- Full Federal Budget

THE CYBERSECURITY CHEAT SHEET

TOP AREAS OF LEGISLATIVE CYBERSECURITY ACTIVITY CONTINUED

Promoting Workforce Training and Economic Development

TRAINING INITIATIVES

States are addressing cybersecurity through the funding of improved security measures and by requiring government agencies or businesses to implement specific types of security practices, including training. Additionally, the government has provided funding towards the training and development of cybersecurity initiatives for individuals through "The National Initiative for Cybersecurity Careers and Studies" (NICCS).

Check out the links below for more information on NICCS and some of the legislation requiring security training:

- The National Initiative for Cybersecurity Careers and Studies (NICCS)
- Cybersecurity Legislation 2018

Threats to Critical Infrastructure

PROTECTING CRITICAL INFRASTRUCTURE

Executive Order 13800 was issued in 2017 and was aimed at modernizing Federal information technology infrastructure to more fully secure critical infrastructure. The implementation of this order was to defend against threats to infrastructure and reduce the national cybersecurity risk.

Get more details on these initiatives by clicking on the links below:

- Executive Order 13800
- Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

TIME TO VOTE!