COMMON d
CYBER SECURITY
NETWORK ARCHITECTURE
REGULATORY COMPLIANCE

Cybersecurity Culture, Control, and Governance

If you shopped at these stores in the last year, your data may be at risk:

- **Macy's**: Shoppers' personal details and, in some cases, credit card information, could have been accessed by a third party
- **Adidas**: "Unauthorized party" said it had gained access to customer data on Adidas' US website
- **Sears**: A "security incident" with an online support partner
- **Kmart:** The retail chain (Owned by Sears Holdings), was also affected by the Sears breach, the company reported on April 4, 2018
- **Delta**: Delta used the same online support service as Sears and was also affected by the reported breach
- **Best Buy:** Third-party for online service, [24]7.ai, and [24]7.ai was compromised by a cyber intrusion
- **Saks Fifth Avenue**: The stores' payment systems were compromised
- **Lord & Taylor**: The stores' payment systems were compromised
- **Under Armour's MyFitnessPal App**: Data was accessed by an "unauthorized party."
- **Panera Bread**: Data leak on its website
- **Forever 21**: Their information may have been stolen
- **Sonic**: A breach of Sonic's store payment system resulted in up to five million stolen credit and debit card accounts being "peddled" in shadowy underground cybercrime stores
- **Whole Foods**: "Unauthorized access of payment card information"
- **Gamestop:** Breach of the website's payments processor
- **Arby's** Malware in the chain's cashier systems allowed unauthorized access

How do you promote a company culture to defend against cyberattacks?

Promoting a culture to safeguard your data is an important role for your organization and a critical component for you to defend against cyberattacks. As an executive of your organization, what do you need to do to promote this way of thinking and introduce this culture of cyber vigilance into your organization? Let's take a look:

Where should you start? Training, training and more training! Employee training should be carried out early and often. Recent studies show that 60% of small businesses breached go out of business within 6 months of said breach.

You should assess, train, and test your employees' knowledge about social engineering techniques. This is not intended to embarrass or punish anyone, but simply to emphasize the importance of being vigilant in a world where attacks are the norm, not the exception.
Create simulated phishing campaigns, with attachments and web landing pages, that exactly resemble the work of cybercriminals and hackers that are likely to attack your enterprise.

Train your workforce on how to spot a phishing email. What do they do with a phishing email? From the results of training and testing, you can track the progress of your phishing awareness program and document improvements.

In addition, your employees should be trained on these topics:

1. How to protect data from your Bring-Your-Own-Device (BYOD)
   From a security standpoint, each mobile device is not 100% secure. Much more work still needs to be done!
2. How to manage and handle removable media
3. How to safely surf the internet
4. What to look for with regard to physical security and environmental controls
5. Social networking dangers:
    a. The do's
    b. The don'ts
    c. The questionables
    d. Email scams
6. Malware: Malware types and their implications:
    a. Adware
    b. Spyware
    c. Viruses
    d. Trojans
    e. Backdoors
    f. Rootkits
    g. Ransomware
    h. Botnets
    i. Logic bombs
    j. Armored viruses

Due Diligence

Understand the current security safeguards for the 3 states of data of your organization:

1. **Data at rest**
2. **Data in motion**
3. **Data in use**

Understanding this can quickly baseline your company's security program.

To understand how your data is governed within the organization, you should have good documentation and a good understanding of the security controls and data governance in place for each of your company's data collection platforms. This needs to be a holistic approach with security program planning and management that provides a framework and a continuing cycle of activity for your organization.

Security Controls

Your security controls should include safeguards and countermeasures to avoid, detect, counteract, or minimize security risks to your system, data, or other assets. They can be classified by the following criteria:

1. **Physical controls**
2. **Procedural controls**
3. **Technical controls**
4. **Legal and regulatory or compliance controls**

To protect the confidentiality, integrity and/or availability of information, the security controls for your organization should include:

1. Security policies and procedures
2. Responsibilities
3. Physical controls
4. Access controls
5. Application development and change controls that prevent unauthorized programs or modifications to an existing program from being implemented
6. Users controls
7. System software controls
8. System services and acquisition controls
9. Configuration management controls
10. System and information integrity controls
11. Identification and authentication
12. Accountability and audit

Data Governance

The term “data governance” is relatively new and heavily-discussed today. There are many different definitions of what data governance is. Most of these definitions are self-serving, but once you look at it in detail, every meaning of the term combines elements of strategy and execution for your:

1. **Data at rest**
2. **Data in motion**
3. **Data in use**

Your data governance program will need to outline the corporate philosophy of your data acquisition, management and archiving. It's an important task that requires both your business and IT sides of the organization to come together to define data elements and the rules that govern data across your users, applications, and your business associates.

To create a safe, secure and sound data governance program with reasonable and appropriate controls, you should have a solid understanding of the following:

1. Your data governance: How do you inventory and manage storage? And who takes ownership of this?
2. Are there processes, policies, and procedure in place to protect, detect, respond to, and remediate threats?
3. Do you have a process to proactively understand and manage cyberthreats?
4. Incident response: Is there a documented plan in place as to how to respond to an incident or suspected incident?
5. Have you done any testing of your disaster recovery process?
6. What cybersecurity crisis management plans are in place? This needs to include and summarize administrative, technical and physical information security controls that safeguard your critical data sets.
7. Have a clear, concise and accurate Information Technology Business Continuity Plan, including a description of any testing in connection therewith.
8. If you work with any business associates, what is your 3rd party exposure?
9. Make sure that your company’s data security governance initiatives have been endorsed by management, including consequences for violations of such policies.
10. How do you manage your risk assessment process?

Once again, promoting a culture that focuses on from the executive team down to all employees to safeguard your data is an important role for your organization and a critical component for you to defend against cyberattacks.

This whitepaper is to help you consider the areas of control and governance that need to be incorporated in your cybersecurity safeguards and provide recommendations as to how to begin the process of establishing a proper security culture throughout the organization.