SECURITY STRATEGY

By: Khalid Diriye

It’s very important to have a plans and phases so including all that into a single framework allows for a quick overview.

The list goes as follows…

1. Management
2. Planning
3. Risk Evaluation
4. Business Impact Analysis
5. Recovery Strategy
6. Data Collection
7. Develop Emergency Center
8. Develop Procedures
9. Awareness and Training
10. Maintenance

FRAMEWORK

- Congregate some sort of IT governance
- Take time out of the work week for security training
- Leverage the use of existing frameworks
- Eliminate third-party risks
- Continue to grow as a company by rewarding those that continue to go above and beyond

RETAIL STORE TASKS

Malware	Trojans
SQL Injections	Worms
Phishing	Man in the Middle

KIND OF ATTACKS

PREDICT ATTACK

- Keep your employees up to date with the latest security threats
- Controlling and keeping private information that may cause harm to your organization
- Keep private information private
- Limits risk and exposure
- Not just for work

- Use logging software figure what exactly can the company lose this includes any classified data, assets (laptops, desktops, tablet, smartphones, etc..)
- Being able to figure where the weak points in your organization are the stepping stones to a more secure feature.

ASSESS RISK

PROACTIVE STRATEGY

- Cyber criminals will use a variety of tactics to gain unprivileged access to sensitive information
  - Phishing
  - Social Engineering
  - Tailgating
- Not all attacks are technical
- You are the first line of defense

1. **Identify and mitigate vulnerabilities**
2. Simulate and analyze attack patterns
3. A robust recovery system

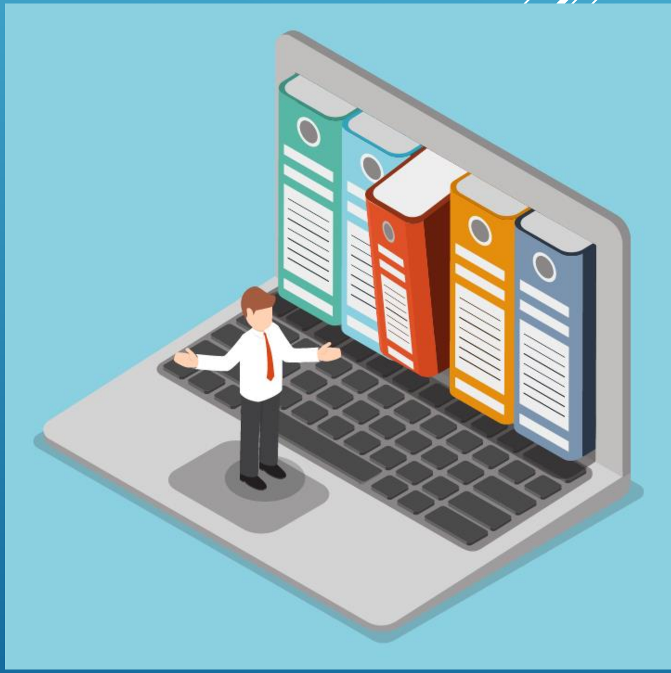
REACTIVE STRATEGY

- Have a step by step plan on how reacting to a situation is done faster, be more effective, and overall have a smoother transition into the next category

- 1. Predict possible damage
- 2. Determine vulnerabilities
- 3. Minimize vulnerabilities
- 4. Make contingency plans

- One of the many key features of a documentation in retail is be able to figure out the 4 following categories:
  - Access
  - Search
  - Possession
  - Transaction

DOCUMENT AND LEARN



- It is very important to be aware of the many tools that can be used in an organization to protect assets from hacks.

- Anti-Virus
  - Microsoft System Center Endpoint Protection
  - Avast
  - AVG
  - Bitdefender (for Android)
  - Avira
- Anti-Malware
  - Malwarebytes

DEFEND AGAINST ATTACKS

- Strong network security.
- Review password policies.
- Review patching routines.
- Review the awareness training.
- Ask employees about the training process.
- Overview financial needs after integration.

REVIEW OUTCOME

REVIEW POLICY

- Reformate any misuse of the market power provision
- Introduce new principles in the planning and zoning rules
- Examine licensing rules with other vendors
- Revision to the policy
- Add on more security measures
- Development plans for the future

- As stated in the previous slide it's very good to be running revision by doing so you are making life easier for the business.
- However many adjustment policies such as a price adjustment policy suffer from abuse that include:
  - Broken items
  - Lost items that are difficult to replace
  - Not publicizing price adjustments
- It is important to keep tracking on what is being adjusted

ADJUST POLICY

- "What Matters Most in Pricing?" Brick Meets Click. N.p., n.d. Web. 28 July 2017.
- "Why Do People Hack?" Regis Information Assurance Programs. N.p., 21 June 2017. Web. 28 July 2017.
- "Contingency Planning: Developing a Good 'Plan B'." Risk Management from MindTools.com. N.p., n.d. Web. 28 July 2017.
- "MSG Management Study Guide." Documenting a Process - Importance and Its Benefits. N.p., n.d. Web. 28 July 2017.

REFERENCES