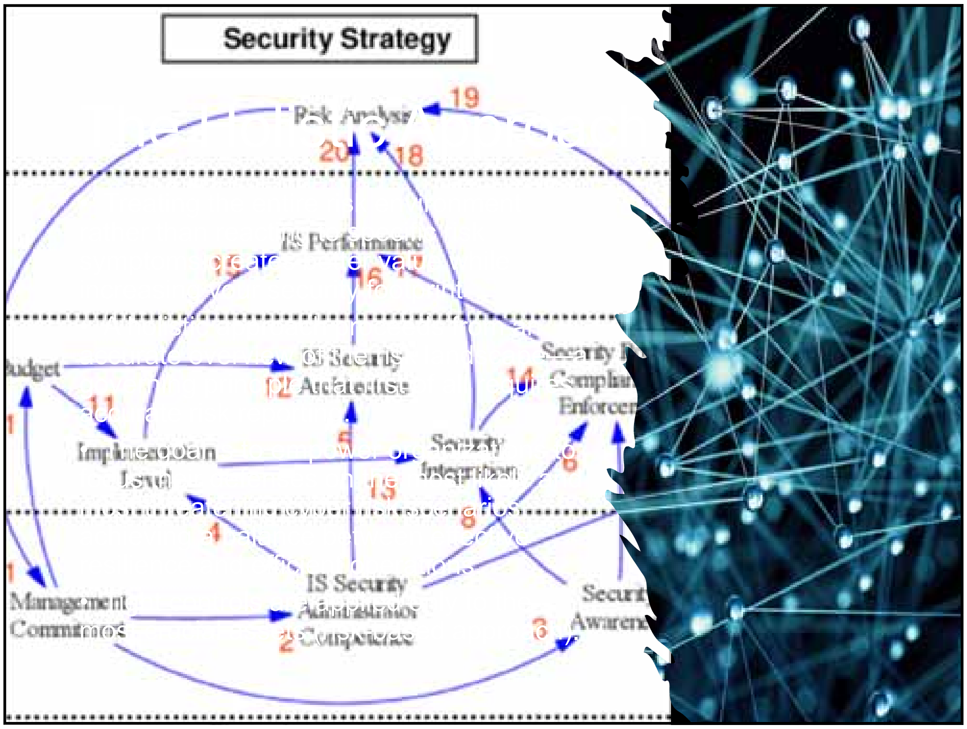
Cybersecurity Planning;
A Holistic Approach

Sponsored by

Heffernan Insurance Brokers

Your Host:
Eric Read
CISA, CISM, CGEIT

The views, thoughts, and opinions expressed in the text belong solely to the author, and not necessarily to the author's employer, organizations, committees or other groups or individuals.



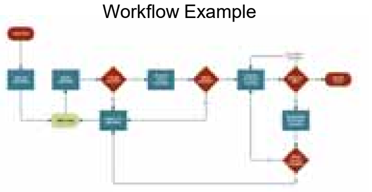
Why the Holistic Approach?

In an IT environment, almost all the systems are connected. This connection may be through direct interfaces, workflow processes or functions which roll up into 10Q and 10K reports.

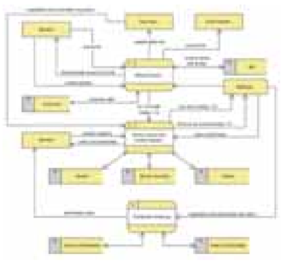
Traditionally, we have looked at each unique system, and rated risk based on the individual system

The Holistic approach looks at systems from a workflow and dataflow view. This allows us to better understand the risks of the unique system, as well as risk that may impact the system from upstream or downstream workflow processes and data flows.

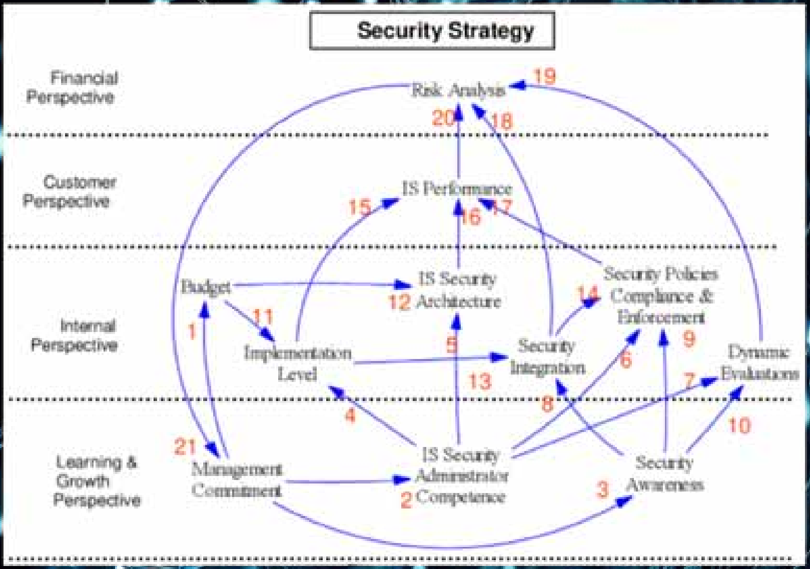
Workflow Example



Dataflow Example



Holistic Security is Hard



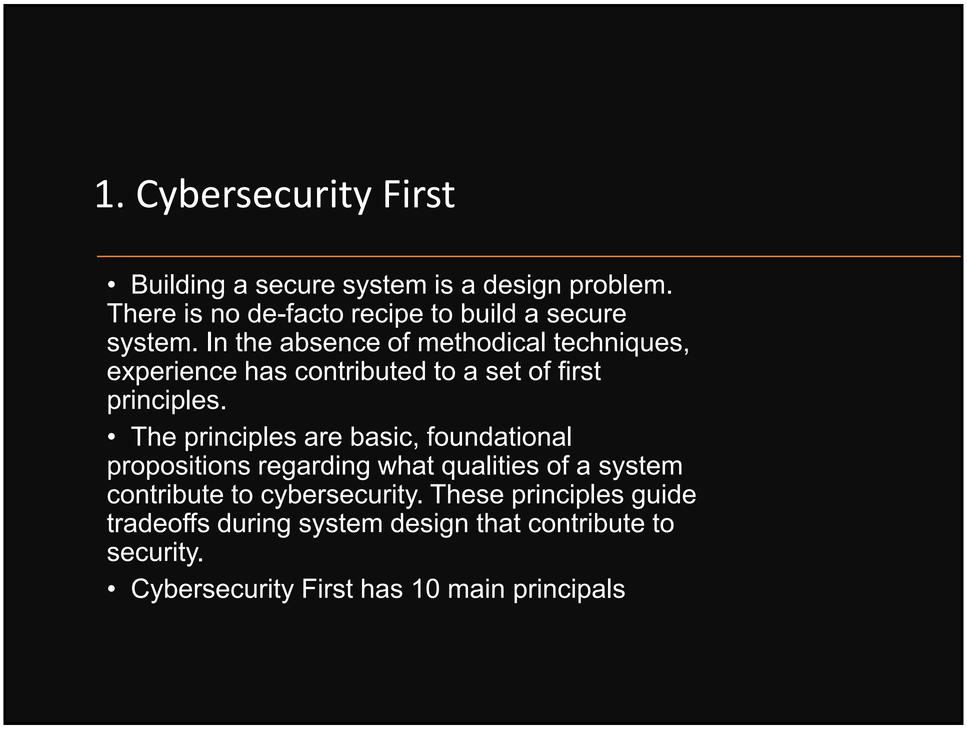
Question 1: Why should we look to a holistic approach for cybersecurity?

a. Risk can be best measured on unique systems

b. The holistic approach is based specifically on workflow

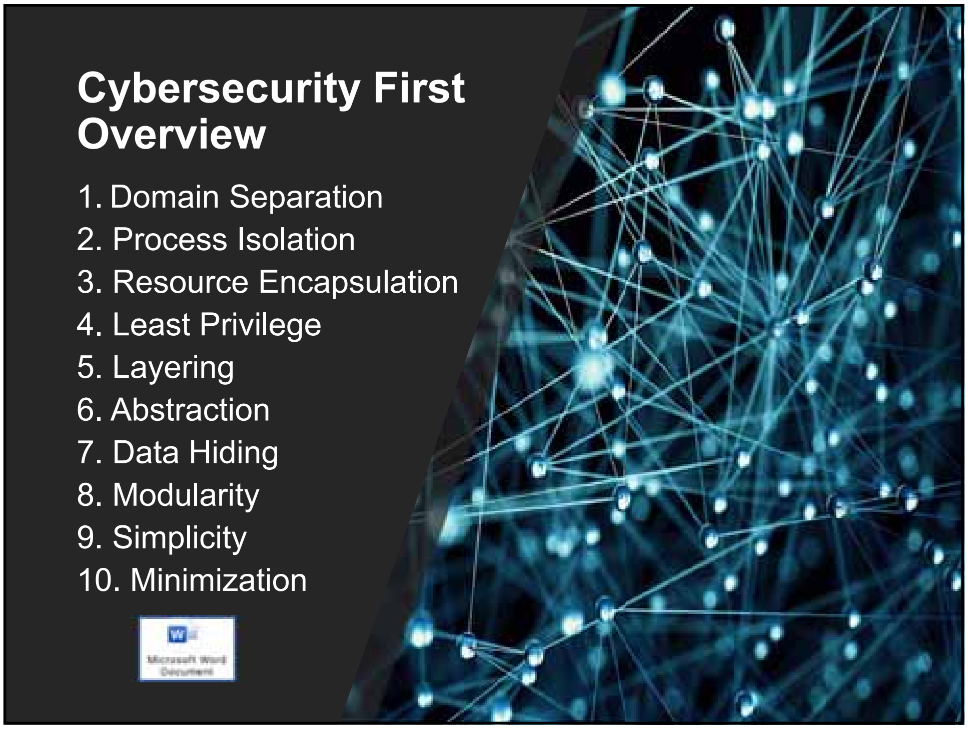
c. Treating the entire risk environment rather than reacting to specific risk symptoms creates better value while increasing your security footprint

d. The holistic approach is based specifically on dataflow



1. Cybersecurity First

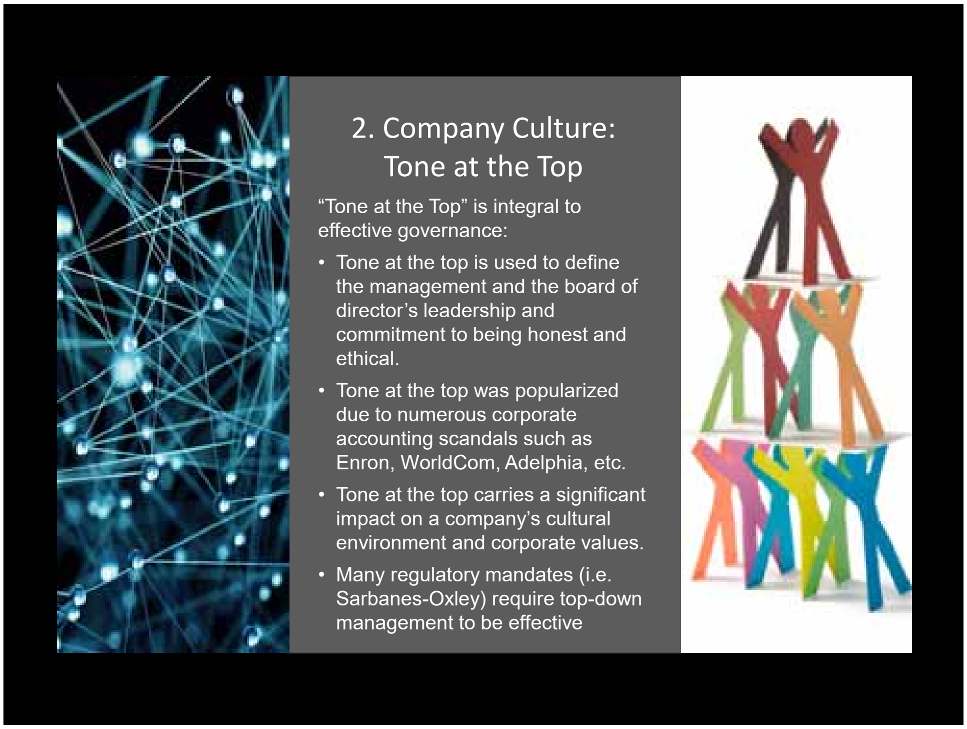
- Building a secure system is a design problem. There is no de-facto recipe to build a secure system. In the absence of methodical techniques, experience has contributed to a set of first principles.
- The principles are basic, foundational propositions regarding what qualities of a system contribute to cybersecurity. These principles guide tradeoffs during system design that contribute to security.
- Cybersecurity First has 10 main principals



Cybersecurity First Overview

1. Domain Separation
2. Process Isolation
3. Resource Encapsulation
4. Least Privilege
5. Layering
6. Abstraction
7. Data Hiding
8. Modularity
9. Simplicity
10. Minimization

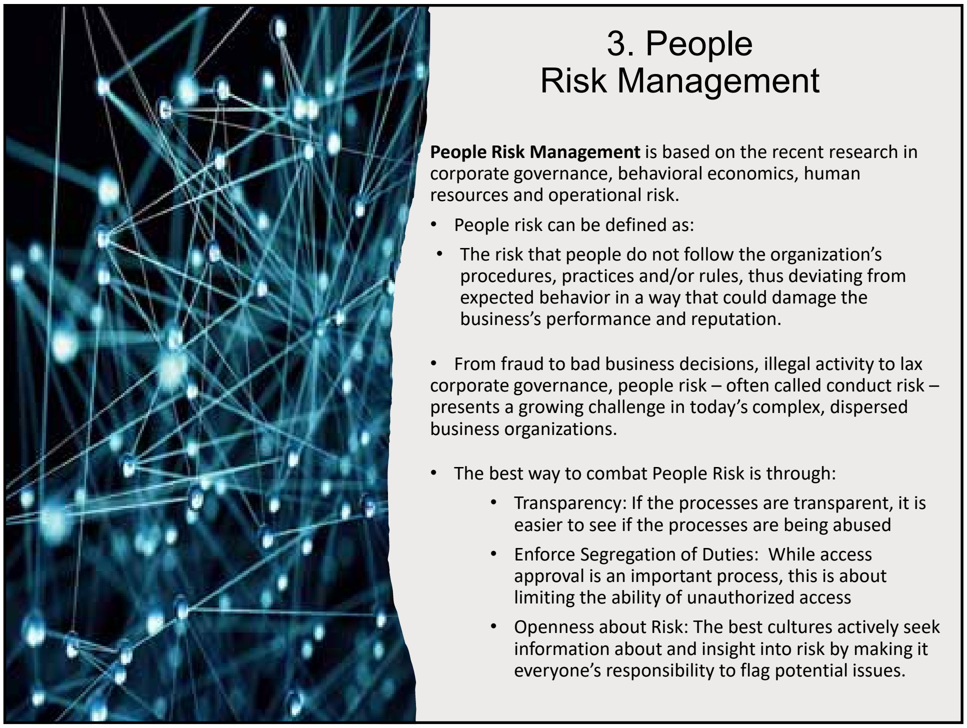
Microsoft Word Document



2. Company Culture: Tone at the Top

"Tone at the Top" is integral to effective governance:

- Tone at the top is used to define the management and the board of director's leadership and commitment to being honest and ethical.
- Tone at the top was popularized due to numerous corporate accounting scandals such as Enron, WorldCom, Adelphia, etc.
- Tone at the top carries a significant impact on a company's cultural environment and corporate values.
- Many regulatory mandates (i.e. Sarbanes-Oxley) require top-down management to be effective



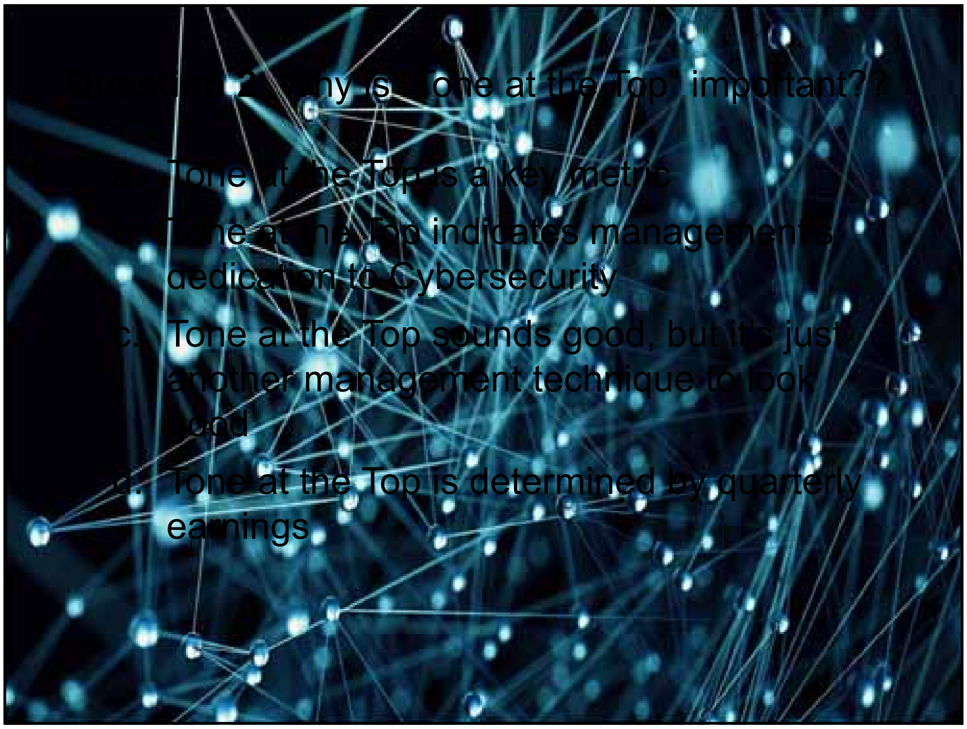
3. People Risk Management

People Risk Management is based on the recent research in corporate governance, behavioral economics, human resources and operational risk.

- People risk can be defined as:
- The risk that people do not follow the organization's procedures, practices and/or rules, thus deviating from expected behavior in a way that could damage the business's performance and reputation.

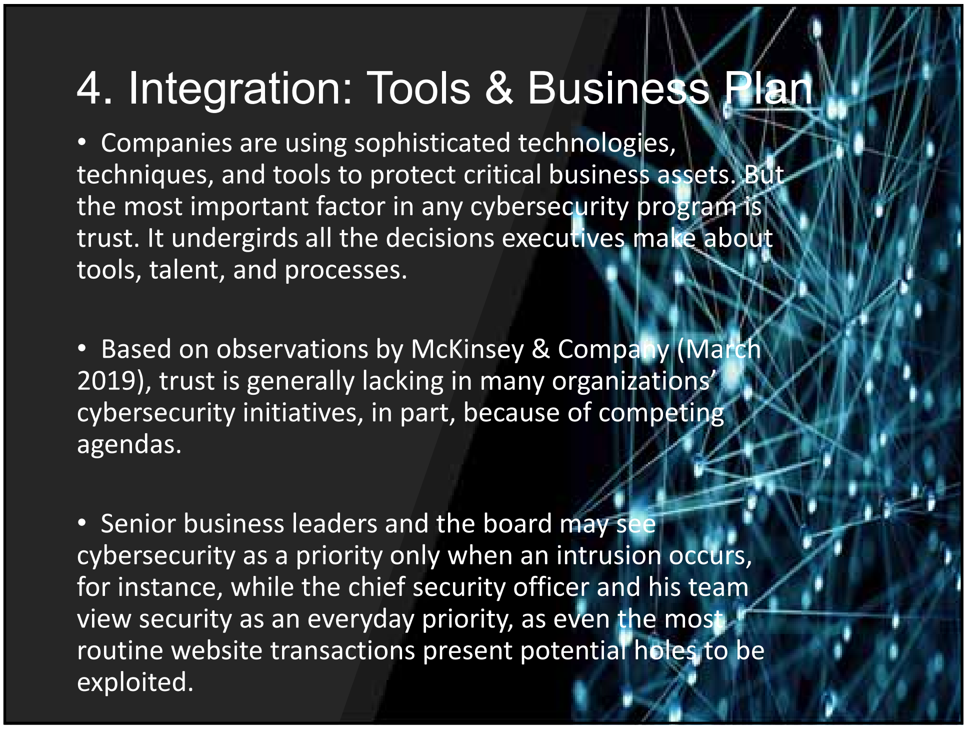
- From fraud to bad business decisions, illegal activity to lax corporate governance, people risk – often called conduct risk – presents a growing challenge in today's complex, dispersed business organizations.

- The best way to combat People Risk is through:
  - Transparency: If the processes are transparent, it is easier to see if the processes are being abused
  - Enforce Segregation of Duties: While access approval is an important process, this is about limiting the ability of unauthorized access
  - Openness about Risk: The best cultures actively seek information about and insight into risk by making it everyone's responsibility to flag potential issues.



Question 2: Why is "Tone at the Top" important??

a. Tone at the Top is a key metric
b. Tone at the Top indicates management's dedication to Cybersecurity
c. Tone at the Top sounds good, but it's just another management technique to look good
d. Tone at the Top is determined by quarterly earnings

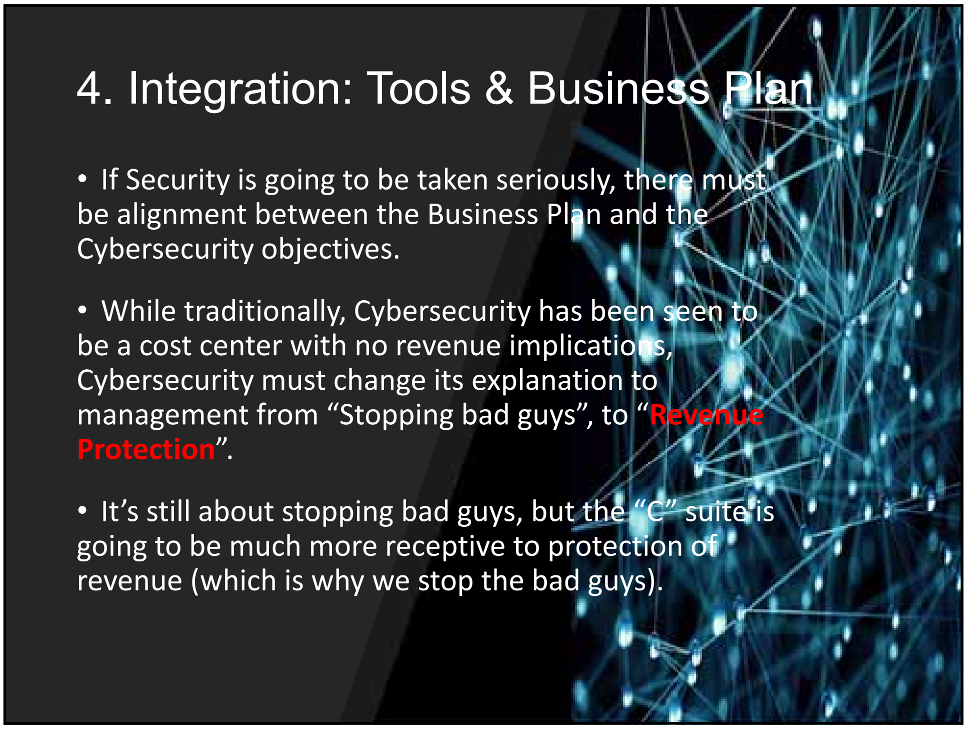


4. Integration: Tools & Business Plan

- Companies are using sophisticated technologies, techniques, and tools to protect critical business assets. But the most important factor in any cybersecurity program is trust. It undergirds all the decisions executives make about tools, talent, and processes.

- Based on observations by McKinsey & Company (March 2019), trust is generally lacking in many organizations' cybersecurity initiatives, in part, because of competing agendas.

- Senior business leaders and the board may see cybersecurity as a priority only when an intrusion occurs, for instance, while the chief security officer and his team view security as an everyday priority, as even the most routine website transactions present potential holes to be exploited.

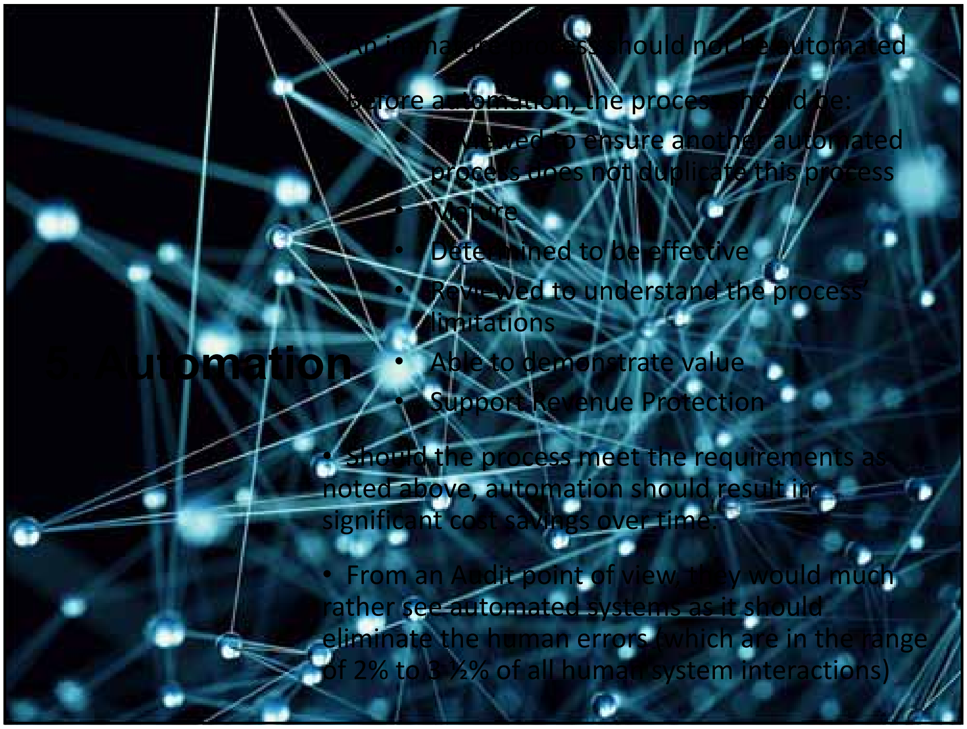


4. Integration: Tools & Business Plan

- If Security is going to be taken seriously, there must be alignment between the Business Plan and the Cybersecurity objectives.

- While traditionally, Cybersecurity has been seen to be a cost center with no revenue implications, Cybersecurity must change its explanation to management from “Stopping bad guys”, to “**Revenue Protection**”.

- It’s still about stopping bad guys, but the “C” suite is going to be much more receptive to protection of revenue (which is why we stop the bad guys).



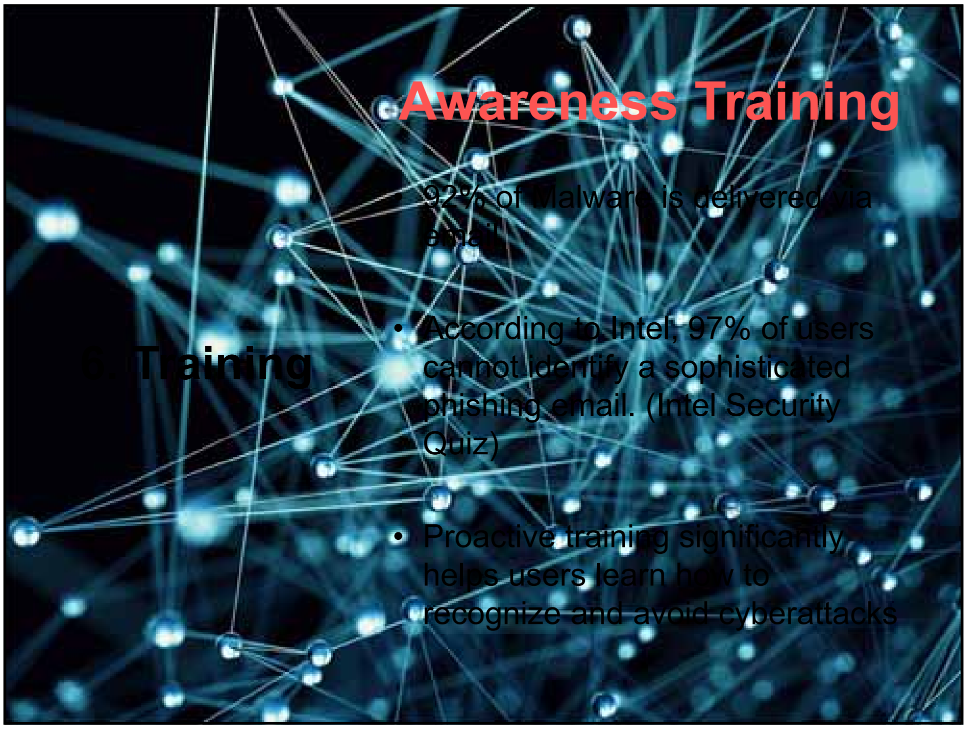
5. Automation

- An immature process should not be automated

- Before automation, the process should be:
  - Reviewed to ensure another automated process does not duplicate this process
  - Mature
  - Determined to be effective
  - Reviewed to understand the process’ limitations
  - Able to demonstrate value
  - Support Revenue Protection

- Should the process meet the requirements as noted above, automation should result in significant cost savings over time.

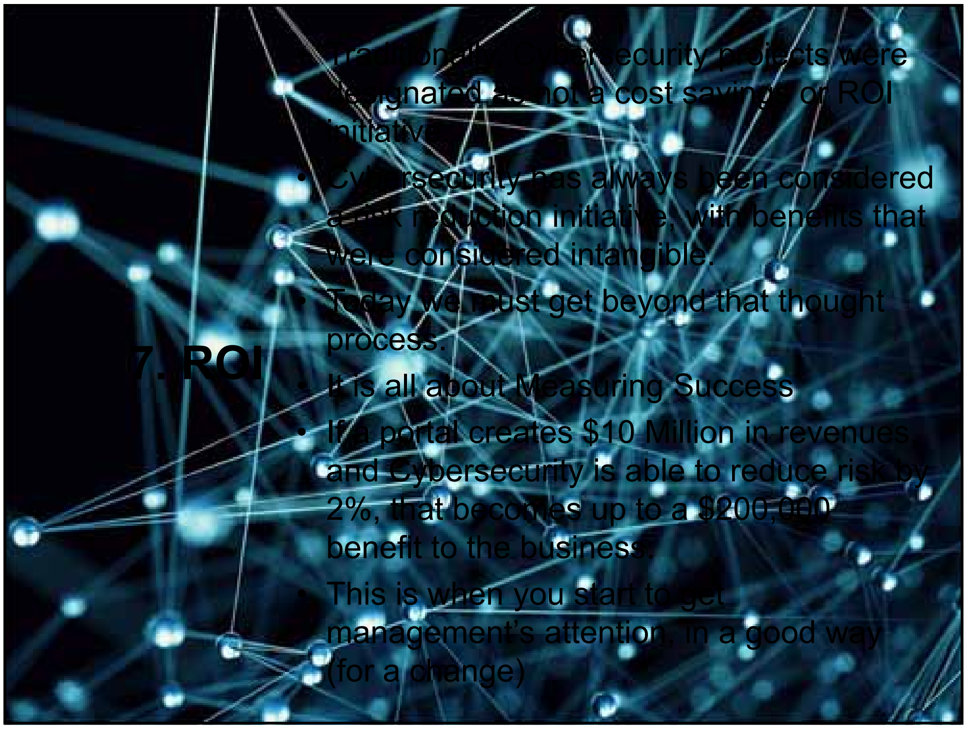
- From an Audit point of view, they would much rather see automated systems as it should eliminate the human errors (which are in the range of 2% to 3 ½% of all human system interactions)



Awareness Training

6. Training

- 92% of Malware is delivered via email.
- According to Intel, 97% of users cannot identify a sophisticated phishing email. (Intel Security Quiz)
- Proactive training significantly helps users learn how to recognize and avoid cyberattacks



7. ROI

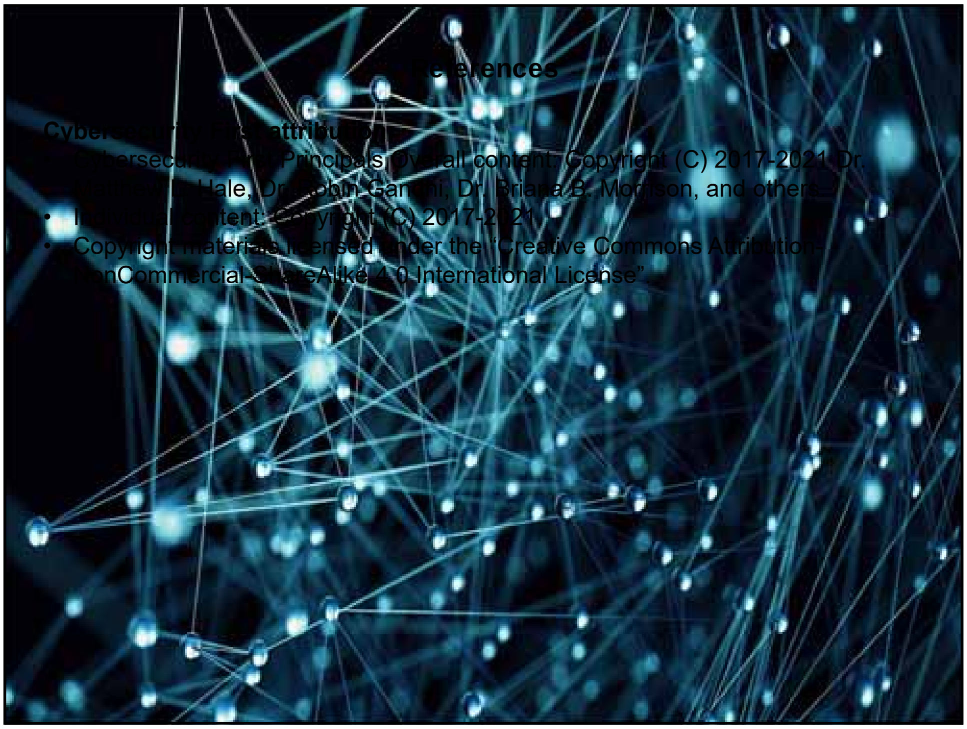
- Traditionally, Cybersecurity projects were designated as not a cost savings or ROI initiative.
- Cybersecurity has always been considered a risk reduction initiative, with benefits that were considered intangible.
- Today we must get beyond that thought process.
- It is all about Measuring Success
- If a portal creates $10 Million in revenues, and Cybersecurity is able to reduce risk by 2%, that becomes up to a $200,000 benefit to the business.
- This is when you start to get management's attention, in a good way (for a change)

Question 3: How do Cybersecurity projects provide ROI:

a. Cybersecurity projects are for risk reduction, no ROI is anticipated
b. ROI is only determined after an incident or breach.
c. ROI is not the concern of the Cybersecurity team. That is a finance responsibility.
d. The ROI is measured by the revenue being processed times the reduction in risk the project provides.

What does this all mean?

- Cybersecurity requires support from the top
- Looking at your system holistically allows a better understanding of your risk landscape.
- Begin looking at KPIs as your friend
- Work closely with your Risk team to demonstrate reductions in risk
- Work with Finance to follow their accepted practices in determining the Business Value of specific instances of risk reduction
- The key term should be “Revenue Protection”



References

Cybersecurity Labs attribution

- Cybersecurity First Principals: Overall content: Copyright (C) 2017-2021 Dr. Matthew L. Hale, Dr. Robin Gandhi, Dr. Briana B. Morrison, and others.
- Individual content: Copyright (C) 2017-2021.
- Copyright materials licensed under the “Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License”.

I hope you have enjoyed our discussion today

If you have questions, I will try my best to provide answers…