Risk, Compliance & Security

SecurIT360
The physics of securing IT

What's the worst that could happen?

Many of us can remember a time when it was common for people to ride in a car without wearing a seatbelt.

In an effort to improve highway safety, statistics were published highlighting the higher rate of injury and death in automobile accidents in which the passengers were not wearing seat belts. Despite the ad campaigns to increase awareness of the risk of not wearing seatbelts, few people changed their behavior, because they just didn't like the inconvenience or discomfort of wearing a seatbelt. Some even argued that seatbelts could cause injuries in an accident. My dad said that he didn't wear his seatbelt because some people had been trapped underwater by their seatbelt and drowned. I always thought that was odd, since we did not live near a significant body of water.

So, if the risk of death or injury did not change behavior, what did change behavior?

Click It or Ticket - Fines for non-compliance.

This is a strong parallel to the way that many companies approach (or do not approach) cyber security. We all know that we face tremendous threats in cyber security, but are we doing what should do, or rolling the dice…

There are many ways to evaluate this, but here is a simple way to assess your company's position on cyber security.

Risk	How much risk are we exposed to by not being compliant and practicing good cyber security?
Compliance	Have we checked enough boxes so that we will not get in trouble?
Security	Have we gone beyond the basic minimums of compliance to practice strong cybersecurity?

If you are doing an honest self-assessment, which one of these positions best describes your company?

In the Electric Utility industry, compliance requirements can vary based on the size of the provider. However, good security is good security, regardless of the size of the company. It is widely known that many smaller utilities do not practice the appropriate level of cyber security. One of the most consistent trends projected for 2017, is that small and medium businesses will see greater threat levels than ever before. That is simply because so many of them are easy targets.

What kind of mindset do you have toward cyber security?

Proactive Mindset	Reactive Mindset
• Measure Risk and Design to Protect	• Minimum Compliance (checklist)
• Monitor for Attacks	• We passed our Audit
• Application Security	• Network Security
• Multi-layered security	• We have a Firewall
• Striving for full Visibility	• We think we have it covered
• Culture of security and continuous improvement	• Want to be compliant and hope to be secure

Believe it or not, those are very real answers to questions that we ask every day.

dburns@securit360.com

Risk, Compliance & Security

SecurIT360
The physics of securing IT

Here is another way to assess your position.

In the cyber security industry, we often use a Control Maturity Model to assess a client's position.

Non-Existent	Never performed, lack of recognizable policy, procedure, or control. Entity was not able to evidence requirement
Ad-Hoc / Initial	Sometimes performed, inconsistent, informal undocumented practice. Entity produced limited reactionary evidence
Partial / Limited	Partially performed, informal, documented practice. Entity produced written evidence supporting requirement (checklists, informal communication, etc.)
Defined	Partially performed, formal policy and procedure, yet to be or partially implemented. Entity evidenced recently approved policy and supporting implementation plan or other documentation
Managed	Consistently performed, formal policy and procedure, fully implemented, recently started. Entity evidenced approved policy and procedure including recent supporting documentation.
Optimized	Consistently performed, fully implemented, operating as expected, at least one review or update period. Entity evidenced supporting documentation of review or update
Not Applicable	Not applicable to the entity

Look in the mirror…

Finally, how would you answer these questions?

- How do you define strong cyber security?
- Do you have strong cyber security policies and practices?
- How would you know if you had a cybersecurity breach?
- What would you do if you suspected that any of your systems had been hacked?

If you do not have clear and confident answers to all of these questions, then you could be exposed to serious risk.

As always, develop a "cyber-defense" mindset and protect yourself.

If you would like to learn more about Cyber Security and how to protect your company, contact -

David Burns
Account Manager, SecurIT360
dburns@securit360.com
205.787.1250