

Cybersecurity programs, Ad Hoc to Mature

Joseph "Dan" Waggoner, CISA, CISSP-ISSAP Director – Cybersecurity

Grant Thornton's global footprint

What you get

- 39 International Business Centers
- Common technology platforms
- Uniform global reporting
- Consistent methodologies
- Common training worldwide









- 1. Collective figures of Grant Thornton International Ltd member firms
- 2. U.S. member firm of Grant Thornton International Ltd
- Including partners



Statistics as of Sept. 30, 2015



Statistics as of Dec. 31, 2015

Grant Thornton's Advisory

CREATE, PROTECT, TRANSFORM.



Create value through Lifecycle M&A solutions tailored for mid-market transactions.



BUSINESS RISK SERVICES

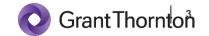
Protect value by identifying, managing and mitigating risk.



transform

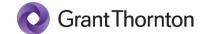
BUSINESS CONSULTING & TECHNOLOGY

Transform value by integrating business consulting and technology offerings.



About Myself

- Involved in IT since 1986
- Involved with IT Security since 1992
- Been with Grant Thornton since 2004
- Has performed SOX, Penetration Testing, IR planning, and FedRAMP/FISMA
- YouTube videos of me dancing with the Magnolia West Fillies (bunch of dad's and the girls performed at halftime)



Why are we talking about Security programs?

- There is more focus on security by the media
- More focus within the business, especially at the higher levels
- The level of interest in this area is growing FAST!
- It is time we mature security and take it to the next level.





Why the need to mature IT Security

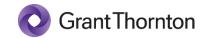
- Security is constantly evolving
- What we have done in the past won't work in the future
- Needs to be business focused
- More education will be needed



Agenda

- Discussion about the three types of programs
 - Whack the Mole
 - Bright and Shiny
 - Adopt a Standard
- A 'mature' standard
 - What does that really mean?





Whack the Mole

Characteristics	Shortcomings
Security issues dealt with, with no plan to reduce instances	Frustration
Security staff experience no growth	Much Easier to be hacked
Long Hours	High Turnover

- Usually performed as the first attempt to become secure.
- May be a part-time 'security' effort
- From the hip, no plan at all



Bright and shiny

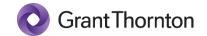
Characteristics	Shortcomings
Security tools bought to address problem	Still Reactionary
No real plan	Wasted Money
Business rarely asked if they need protection	Lack of planning

- We can buy what we need, to address the issue of the day
- Pen Test also fall into this category
- Can be costly



Penetration Testing

- What it is, and isn't
- What you need to see on a Pen Test
 - Methodology
 - WHO did the work
 - Manual Testing
- PCI Guidance on Penetration Testing
- FedRAMP guidance on Penetration Testing



Adopt a standard

Characteristics	Shortcomings
Rarely a business desire to use a standard	Every Standard has gaps
One Standard used	Not business risk based
It is NOT bad, but not where you want to be	Someone else decided what should be done

- Not always using a standard, may be a list of risks
- Rarely is there a plan to implement
- Even adopting a standard you can be compromised



Clues that you have an immature process

- Business not involved in making the plan
- No documented plan (think about your audit plan)
- High staff turnover
- Frustration at all levels, including outside of the Security Department
- Always seems to be a fire drill of some kind happening



What does a mature security practice look like

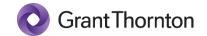
Characteristics	Shortcomings
The business is involved in determining what needs to be protected	Requires more effort
Has the characteristics of all three	Requires more money to be spent
The plan is always evolving	Not many!!!

- Not just one person deciding
- Takes the right controls from the right area to address the right risk
- Not tied to just one standard
- Constantly evolving



Clues that you have a mature process

- Business involved in the Security Process
- There is a documented plan going forward
- There is a governance program
- There is a security budget with variance measurement
- Rarely is the business subjected to a fire drill because of a security issue



Auditing the plan

- Determine who has been involved in determining the risk and how to address them
- There is a documented plan that you can audit, they may need to make changes but it should be documented and justified
- They don't compare themselves to peer but see if they have improved from the prior year (continuous improvement)
- There is a budget for the security, and it is properly managed
- They have established KPIs to determine if the plan is working as intended



Closing

- The three type of programs you don't want
- The one type we should strive for
- Questions?



