DEATH BY CHECKBOX:
PUTTING ANALYSIS BACK IN THE ANALYST

SHELLY EPPS, MS, HCISPP

Disclaimer Slide

Disclaimer:	What follows is a solely my opinion and is not intended to represent views or practices of current or former employers or any organization I am or have been affiliated with.

2nd Disclaimer:	Use of images from the internet with reference when available. No infringement intended.

3rd Disclaimer:	I have absolutely no idea how legally binding either of the above disclaimers are.

Challenges:

Most institutions do not have the bandwidth & scalability within their security teams to do individual risk assessments on every vendor and system even once, let alone annually.

Procurement/Contracts execute security terms that they often do not understand. Security analysts often do not read or understand contracts.

Desire (rather than business need and efficiency) often drives purchase. Intake funnels are difficult to control resulting in limited visibility.

Documentation is often lacking, instead replaced with assurances that vendors are safe/secure/compliant and that other similar organizations are already using them.

Requested review turnaround is ASAP. Experienced security analysts are hard to hire and may not be interested in the “less technical” aspects of InfoSec.

Need for metrics to justify ROI for enterprise risk assessments & roadmapped security initiatives.

Where does that leave us?

Queues may be backed up months in advance. Security is perceived as being a barrier = angry customers.

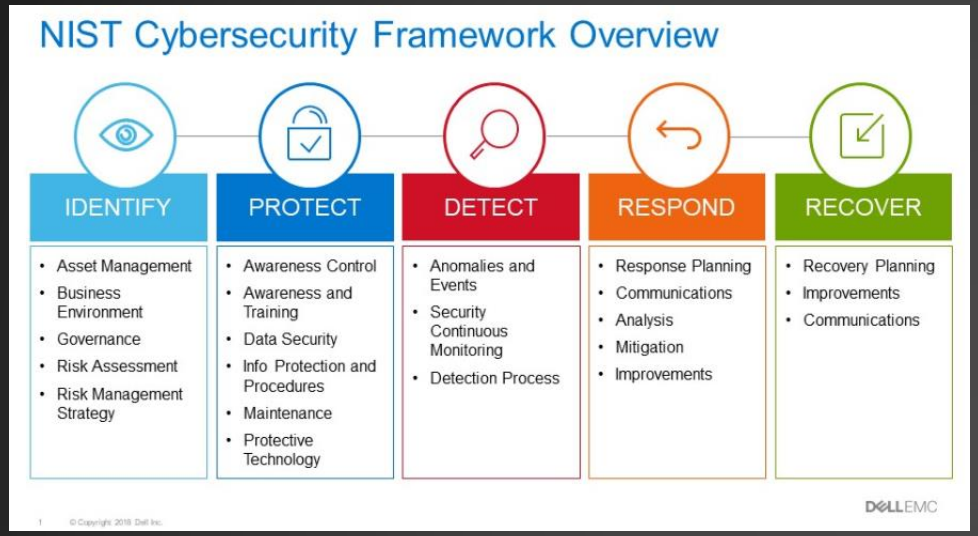
Multiple systems are purchased for identical scopes of work (e.g., calendaring tools, surveys, cloud hosting, file sharing).

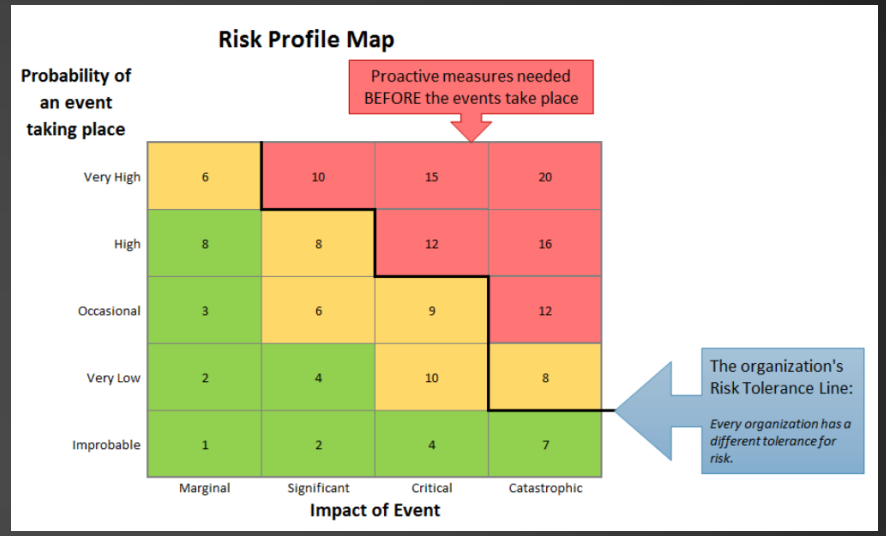
“Shadow purchases” that do not get assessed (e.g., low dollar amounts, click agreements).

High security analyst turnover – it’s a seller’s market!

Continual re-creation of the wheel.

STANDARDS, FRAMEWORKS & CHECKLISTS…OH MY!





Inevitably, to survive, we adopt an IT framework, work on inventory and asset management, categorize assets using heat maps, determine risk tolerance, standardize questions, purchase a risk/governance software, likely hire project managers, tighten funnels and begin wrapping our arms around the task of systematically and consistently securing an organization that is constantly under attack. We collect lots and lots of data that inform our risk.

And every bit of that is exactly what an organization should do, but…….

THERE'S A REASON IT'S CALLED A SECURITY "ANALYST"

This is not good

The unintended side effects of absolute standardization can be that you strip the analytic process right out of your highly paid analysts, retraining them to either think only within the pre-defined parameters you've set – or - you lose good talent when they get bored.

Reviewing vendor provided questionnaires (or 3rd party audit reports) and writing a report is going to check a box that needs to be checked, but it may leave you with gaps that a few, targeted questions from an experienced analyst could identify and/or address.

This is even worse

HYPOTHETICAL EXAMPLE 1: ENCRYPTION

AT REST

- Question: Are all data encrypted at rest on mobile devices using industry standard encryption? Yes/No
- Questionnaire answer: Yes
- Final answer: ummmm, No

IN TRANSIT

- Question: Are all data encrypted in transit using industry standard encryption? Yes/No
- Questionnaire answer: Yes
- Final answer: Nope

HYPOTHETICAL EXAMPLE 2: FILE SHARING

DATA SENSITIVITY

- Question: Categorize the sensitivity of the data that will be disclosed
- Questionnaire answer: Deidentified data
- Final answer: Fully identified data

ACCESS

- Question: Is access provisioned based on principles of minimal necessary and least privilege access? Yes/No
- Questionnaire answer: Yes
- Final answer: No

HYPOTHETICAL EXAMPLE 3: BUSINESS CONTINUITY

WORKFORCE

- Question: Do you have a designated individual responsible for security oversight of the organization? Yes/No
- Questionnaire answer: Yes
- Final answer: Kinda

BACKUPS

- Do you have backup systems that are tested on at least an annual basis? Yes/No
- Questionnaire answer: Yes
- Final answer: Not for you though
- Alt Final answer: Yes, but you won't like where they are.

FINAL HYPOTHETICAL EXAMPLE

DIAL IT DOWN A NOTCH

• Categorize Sensitivity of the data:	Sensitive/Identifiable
• Do you have a company 3rd party audit:	No
• Recommend Approve/Deny	Deny
• Final Recommendation	Approve with no 3rd party audit requirement – because it's overkill based on the SOW and other mitigations would greatly reduce the risk

THERE'S A REASON IT'S CALLED A SECURITY "ANALYST"

Do you want to use consistent, standardized security questions, decision trees, and generate useful metrics/data?

Do you want to be free to follow threads, ask open ended questions, and use intuition and experience?

QUESTIONS?