RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **RMG-M06**

How to Win with Cyber Insurance & Sidestep the 7 Biggest Pitfalls

Cynthia James

Enterprise Security Executive
Microsoft Cybersecurity Solutions Group
cynthia.james@microsoft.com

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

My personal disclaimer: I am not an insurance agent! Please confer with one before taking any suggestions I make, as per above. This presentation is meant to help you combine industry survey results with a risk multiple that *may* help you ascertain a useful level of coverage, but this represents my **opinion only.**

Special thanks to my reviewers/collaborators (any errors are mine): Patrick Hellman, CISO at Arrow; Richard Hobson, UK Global Broking Group; Tara Knapp, Microsoft

Microsoft

Agenda

- History of Cyber Insurance & Challenges Estimating Risk
- The Best Way to do It
  - The CISO's Role, Steps to Take
- Tools to Get it Done & Sample Estimations
- Caveats, Gotchas & the Top 7 Pitfalls!

RSAConference2022

The State of the Industry, Challenges, Estimating Risk

Recent history, what's covered

History: the Cyber Insurance Industry

- 2017 – “we just want to be in the cyber market”
- Inexpensive add-on by agents with no cyber-knowledge, no security questions
- 2021:
  - $20B market
  - But a very poor “loss ratio”
  - Lloyd’s: “no more silent cyber”
- 2022:
  - “costs are up and more hoops to jump through” (CISO quote)
  - larger companies get multiple bids; on-site checks
  - Sublimits come into play (“up to $100K for X expense”)

Cyber war exclusions – “collateral damage”

- Cyberwar: "the use of physical force by a state against another state … whether war was declared or not."
- The term "cyber operation" is defined as "the use of a computer system by or on behalf of a state to disrupt, deny, degrade, manipulate or destroy information in a computer system of or in another state.“
- Protections:
  - don't speculate on attribution
  - get your own sources legal counsel if necessary

*Cyber Insurance and War Exclusions (darkreading.com)

What's coming?

- Increased rates, specific security capabilities
  - standardized scoring?
- Do cybersecurity companies offering warranties actually pay?
- "External view" vs "internal view" of security?
  - Will there eventually be premiums which fluctuate according to scores?

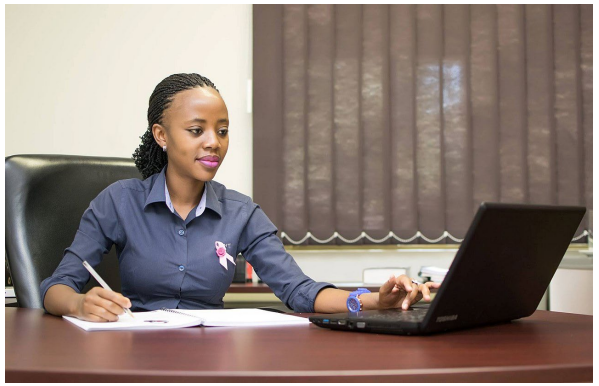
		Likelihood Score	Vulnerability Score		
Likelihood	High	3	3	6	9
	Medium	2	2	4	6
	Low	1	1	2	3
Impact Score			1	2	3
			Low	Medium	High
			Impact		

Known Challenges – how do Insurance companies estimate their risk?

- No reliable actuarial tables – fluctuations can be extreme
- Cybersecurity posture can change from “positive” to “disastrous” in seconds
  - Who else’s cybersecurity is in the mix? (i.e., SolarWinds)
- Cyber isn’t a building or an earthquake
  - It may come closest to an adrenaline junkie getting life insurance

Interacting with the insurance company

- Who to reach out to during an incident and what are time constraints?
- How often must we report our cybersecurity posture, and what constitutes proof?
- How does scoring last year compare to this year?



What insurers help with

- Usually:
  - Ransomware negotiation and remediation
  - Notification costs
  - Costs to restore & recover data – (you should have a prioritization schedule)
  - Forensics – what exactly happened (ascertaining fault, attribution)
  - Loss of immediate income
- Often:
  - Ransom (extortion) payments – maybe with sublimit
  - PR and marketing related to brand management/damage
  - Customer attrition (how measured? CMO question)

Almost Never

Long term effects

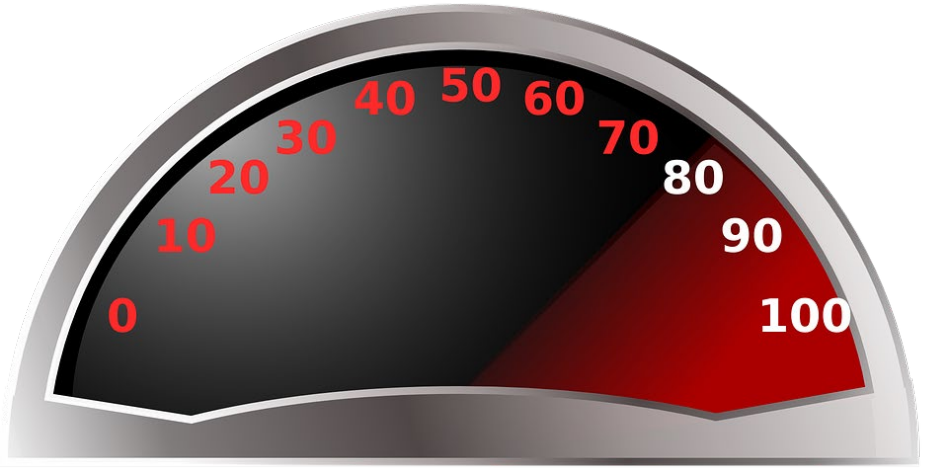
- Brand damage
- IP – the damage involved in having secrets shared
- Security upgrades in the aftermath
- Acts of cyberwar

The details of coverage

- For what period will expenses be paid? Long tails
- Will they consider your investments? (table tops & DR planning)
- Beware attribution!

Determining coverage: bracketing

- Top down: protect the full value of the company?
  - Reasonable for a small company?
- Bottom up: protect based on the probability of threats, the cost of repairing the damage , what threats you are most susceptible to
- This middle ground = gushy, but let's take a shot!



Summary of 5000 mid-sized companies, 2021

- 95% of claims were paid
- 70% of the time insurance providers paid biz recovery costs
- But: “We don’t pay for losses due to outdated or unsupported systems”, etc.

RSAConference2022

The Best Way to Do It!

Where the CISO comes in

The CISO's involvement is critical

- Finance, Legal & CEOs rarely understand cybersecurity
- CISOs are the only ones who can:
  - Estimate the risk of breach & impact
  - Review sublimits & exclusions
  - Know what tech requirements can be met
  - Manage the recovery process (in alignment with the policy)
- The CISO should be involved in deciding how his/her team spends their time
  - Reporting scores & tracking compliance

What else is the CISO* uniquely able to do?

- Answer the questions: 17 cyber insurance application questions you'll need to answer | CSO Online *
- Will DR planning help reduce costs? What about BCP, BIA?
- Estimate recovery (time, spend)

* or top security officer

3 levels of analysis – how much time do you have?

1. Quick: a few hours
   - Estimate cost & probability, + 4 critical risk factors
2. Weeks/month
   a) Is there acceptable, alternative biz continuity? (low-tech or virtual desktops)
   b) How secure are your users, suppliers, partners?
   c) What is typical posture for your industry?
3. 3 months or more – dig in & collaborate internally until you reach diminishing returns (BCP, etc.)

Summary

- At the very least – review the current policy
  - Who are your contacts in case of an incident, timing rules?
  - What are security scoring & reporting expectations?
  - What is covered and for how much?
- Gather the numbers, share, commit to scoring and/or new tech
- Work the politics
- **Ask for more cybersecurity budget!**

RSAConference2022

Tools to Get it Done

…and a Sample Case

Pop Quiz re Colonial Pipeline ransomware

- What Russian group was it attributed to?
- How much was the ransom?
- If you have THIS enabled on your PC, some Russian malware will by-pass you.

Lots of squishy numbers!

Ransomware Probability	Data Breach Probability	Cost	Other Cost components:
• Low - Sophos, 2021 = 51% hit; 50% of those were successful → 25% risk • Medium - IDC said in 2021 **37% were hit** with medium level severity • High – 47%	• Low - Varonis, 2021 = 27%, 50% severe → 13.5% risk • Medium - Ponemon & IBM say **28% probability** of a "successful moderate level attack"	• Low – Coveware, $6K for small company • IBM/Sophos says average cost **data breach $4.24M**; **ransomware, full recovery $2.8M** • High - Ponemon & Proofpoint, 2021 "large US companies" $14M on average	• Personal data up to $380 for Healthcare; IBM/Ponemon = **$180 average per record** • Average ransom: **$170K** • Average **BEC loss $183K** (FBI says $108K)

Note: it's very hard to find a study NOT done by a cybersecurity vendor!

Microsoft

Quick & Easy, Expectation of Incidents & Cost*

Incident Type	Cost	Probability/#	Total Expected	Total Potential
Ransomware	$2.8M	37%	$1.04M	$2.8M
Data Breach	$4.24M	38%	$1.61M	$4.24M
Personal Data	$180	1K records	$180,000	$180K
BEC	$183,000	1x	$183,000	$183K

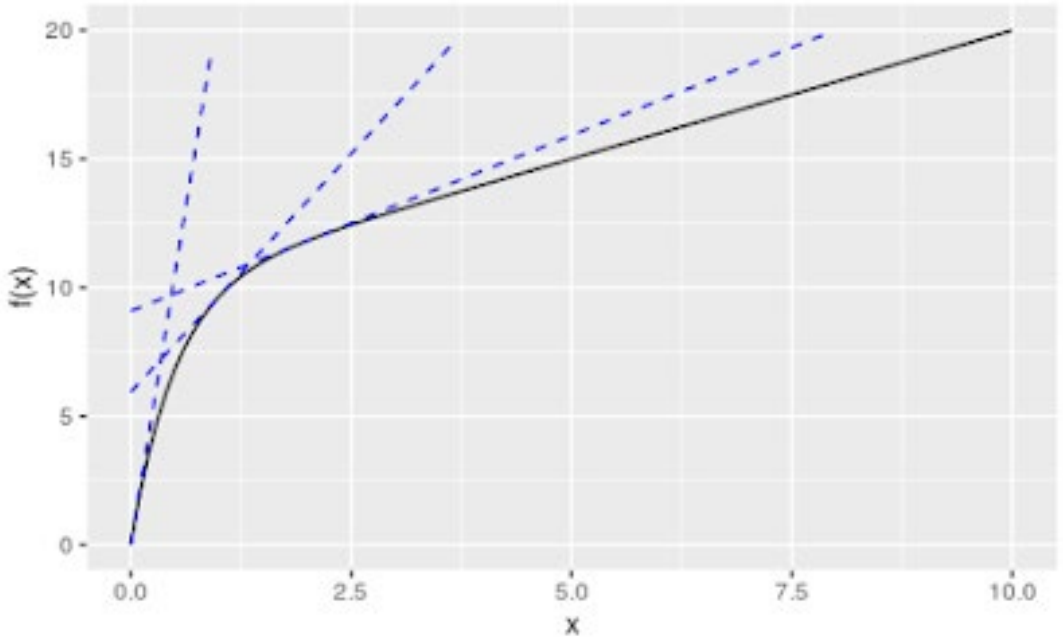
Expected	Potential
$3,013,000	$7,403,000

Opinion Question: Does $3M seem like an okay absolute minimum?

* Sophos, IBM&Ponemon, Varonis

Insurance/Company size: not a linear function

- Smaller companies need more protection relative to their total company value
  - A catastrophic incident *may* bankrupt the company
- Suggest: Companies from $1M - $20M need to insure themselves for close to what they are worth
- $500M companies don't need to insure for their value



Microsoft

Where we are headed

Inputs:

- **Baseline Risk in $ = [Probability x Cost of Risks]** - $3M
- **Incident Sensitivity Multiplier = [4 risk factors]** – 1x? 2x?

Baseline (min insurance) x ISM = $suggested insurance

What was my disclaimer at the beginning? I am NOT an _____?

A Method to Measure Sensitivity to Incidents

- Incident Sensitivity Multiplier: Identifying 4 of the biggest factors
  A. Reliance on technology to run the business (downtime hurts)
  B. Customer sensitivity (likeliness to sue if data is compromised)
  C. Confidence in ability to recover (tested off-line backups, etc.)
  D. Confidence in cybersecurity posture (the basics: vuln scanning, MFA, etc.)
- Suggested: a simple point system to calculate a multiple of the probable loss number, aka your **Incident Sensitivity Multiplier**

Table 1: how expensive will a failure be?

(1 is best)

Factor	Low	Medium-Low	Medium	Medium-High	High
Reliance on Tech (revenues)	1	1.25	1.5	1.75	2
Customer sensitivity (likely to sue?)	1	1.25	1.5	1.75	2

Climbing Gym

Table 2: How good is your cybersecurity and your ability to recover? (1 is best)

Factor	Low	Medium-Low	Medium	Medium-High	High
Confidence in Recovery (backups, tested, off-line)	2	1.75	1.5	1.25	1
Confidence in Posture (MFA, VPN, patching)	2	1.75	1.5	1.25	1

Two main factors, inversely related (1 is best) (this table = a perfect score)

Add it up, divide by 4 to get incident sensitivity quotient (sample #s only)

	Solutions	Low	Medium-Low	Medium	Medium-High	High
A	Reliance on Technology	1	1.25	1.5	1.75	2
B	Customer Sensitivity	1	1.25	1.5	1.75	2
C	Confidence in Recovery	2	1.75	1.5	1.25	1
D	Confidence in Posture	2	1.75	1.5	1.25	1

How do these number affect each other?

Rule:

- ✓ Add all 4 numbers, divide by 4 and multiply the resulting number by the Probable Loss to get a number that reflects Incident Sensitivity

This gets us to an **Incident Sensitivity Multipler**

One way to use it:

Climbing gym: 1 + 1 + 2 + 2 = 6/4 = 1.5 x $3M = $4.5M minimum insurance by Q&D method (Climbing Gym, 1/5 or 20% of the value of the company)

Pop Quiz

- What year was Stuxnet discovered?

Adjusting the Model to Fit Better

Three things can easily be changed:

1. **The baseline number (= minimum coverage)**
2. **Incident Sensitivity Multiplier: what is the spread? This can be derived from internal opinions; what does Risk/Finance/CEO think it should be, max/min?**
   - **This table = 1-2 but internally if they want to go much higher, include that in the spread – i.e., 1x to 5x / example: $10M - $50M – if scores on all 4 factors are poor, 5x is the coverage**

Scores for the 4 factors of Incident Sensitivity

Rule:

Add all 4 numbers, divide by 4 and multiply the resulting number by the Probable Loss to get a number that reflects Incident Sensitivity

Incident Sensitivity Multiplier

Hypothesis: **when** the multiplier reflects an appropriate level of insurance, it can begin to bring some rigor to the process and **can be adjusted over time** as attack conditions and costs change.

However: always confer with an agent on whether the output is reasonable in your specific case – consider breaking down agent recommendations to fit the model. Always take a bigger baseline if it's an option!

*Richard Hobson: "**Buy as much as you can afford – take the number you think you need & double it**."*

Other ways to go about it

- Additional possibilities:
  - **Add 10-20% of annual revenue** – for biz interruption to be included
  - **Insure to full value of the company** – the potential for catastrophic loss
  - **Use full potential cost as baseline**

Agent: "I recently had a client renewal with existing policy limits of $5M that was only offered $3M at renewal. They had no losses but their deductible went from $5,000 to $25,000. Their premium went up 5x!"

More Tools

- Biz Continuity (keep it going – before/during/after financial viability) : Business Continuity Plan: A Complete Guide (sweetprocess.com) ←protects against ALL disasters Business Continuity Plan | Ready.gov
  - Reminder: Biz Cont Plan = a.) Biz Impact Analysis; b.) Disaster Recovery
- BIA guidance (NIST) sp800-34-rev1_bia_template.docx (live.com)
- Biz Impact Analysis Business Impact Analysis | Ready.gov (predicts consequences, gathers data needed to recover)
- CIA ranking (healthcare vs banking vs power co) – ransomware = loss of availability at least, some integrity; data breach = confidentiality
  - Asset valuation: Risk Assessment & Control Implementation Model | ISACA Journal
- Quantification of Cyber Risk for Actuaries An Economic-Functional Approach (soa.org)
- Disaster Recovery (get it back up): a component of Biz Continuity IT Disaster Recovery Plan | Ready.gov

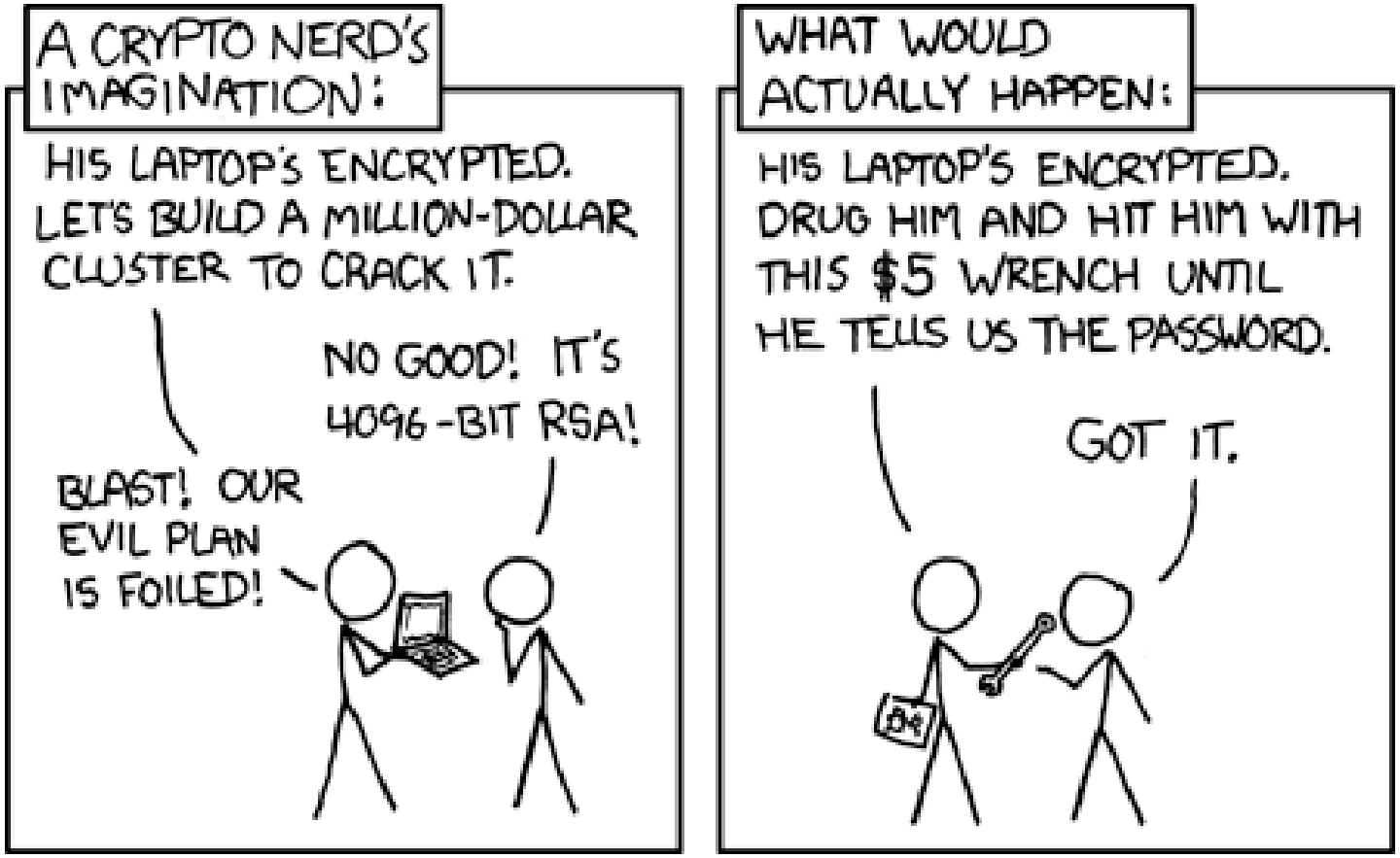
Security to spend on – visible to insurers

- MFA
- Phish-testing users
- DR set up (off-site backup at least), tested
- Coordinated end-point protection + cloud risk management – (comprehensive alerting system); Managed Detect & Respond (external support managing threats)
- Encrypt sensitive data
- Enforce Data Loss Prevention, data labeling, etc.

Helping Finance/Legal Understand

- **What makes cyber special & different?**
  1. Extreme **asymmetric attack advantage** (one good Zero Day in the hands of one good hacker can lay waste to hundreds of companies in days)
  2. **All software and hardware** has weaknesses (**Zero Days**)
  3. 24 years of experience shows: constant evolution in **cybercrime** innovation, **leapfrogging protection** efforts
  4. Cybercrime innovation gets shared real-time with criminals via researchers, protective patches – **constant, brilliant innovation for free**
  5. AND we can't run business with no humans and fully air-gapped from the internet ←the routes by which all cyber risks travel

xkcd


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Getting What You Want

Listen first.

If that's not possible (grumpy Finance!): offer 17 questions, scoring requirements, tech requirements, protocol to follow post-incident, "let's meet again"

Do NOT offer numbers without getting theirs first.

RSAConference2022

Caveats, Gotchas and the Top 7 Pitfalls!

The top reasons insurers don't pay

1. "It's related to the same breach as last year"
2. "We only pay up to _____" (sublimit)
3. "We only pay for costs AFTER you notify us"
4. "We gave you negotiators/forensics/media advice you didn't use"
5. "Your depiction of your security posture was inaccurate"

Microsoft

The Fine Print…be sure to track security compliance

- Comply with reporting/scoring expectations
- Report scores as agreed upon
- What else is in the contract?
  - This is where the risk folks & legal can help
- BTW…has HR followed through on every background check? (insider risks)

The 7 Biggest Pitfalls – quick list

1. Not getting enough coverage
2. Not being explicit with coverage (no silent cyber)
3. Not socializing estimations (get the history first)
4. Committing without knowing the required posture reporting
5. Sharing too much with the insurance company
6. Auto-renewing without a price check & re-assessment
7. Not ensuring that all critical threats are covered

The 7 Biggest Pitfalls/Errors

1. Not getting enough coverage
   - Consider any cost-reductions they make available (scoring, tech)
   - Get competitive bids
2. Not being explicit with coverage
3. Not socializing tradeoffs, estimations & expectations
   - Being ignored by Finance/Legal
     - Don’t end up the scapegoat!
   - Document your suggestions

The 7 Biggest Pitfalls/Errors – continued

4. Over-committing or under-committing to reporting
5. Sharing too much or too little
6. Don’t renew a policy without:
   - Reevaluating pricing & the threat environment
7. Not ensuring that all critical threats are covered (use scenarios)

Apply What You Have Learned Today!

- Next week you could:
  1. Get a copy of the current cyber insurance policy
  2. Analyze according to this presentation (caveats, requirements, coverage level)
     - Query insurance agent as necessary
  3. Suggest a meeting to **Listen First** and discuss findings
- In the next 3 months following this presentation you could:
  1. Meet with peers and management to get a good idea of Biz Continuity needs (and help them understand cybersecurity issues better!)
  2. 2nd meeting, clarify where the current policy falls short or what it would take for it to fit (boost cybersecurity investment!)
  3. Request resources/budget to accommodate & put a plan in place

END

Thank you!

Special thanks again to my reviewers/collaborators (any errors are mine): Patrick Hellman, CISO at Arrow; Richard Hobson, UK Global Broking Group; Tara Knapp, Microsoft