2018 Secure360 Twin Cities

Five Ways to Improve Your Cyber Risk Communications

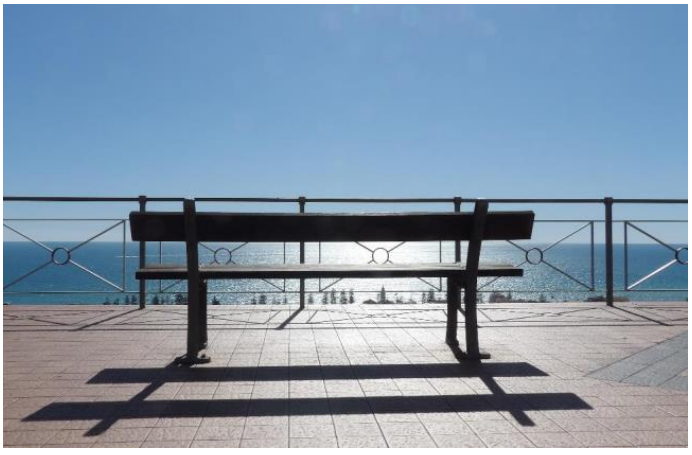
May 16, 2018

Christophe Veltsos
aka @drinfosec

SECURE360 conference

Five Ways to Improve Your Cyber Risk Communications

Chris Veltsos aka @DrInfoSec



Agenda

- Why are boards asking cyber-related questions?
- What type of questions are they likely to ask?
- How do dynamics in the C-Suite foster/hinder conversations? Strategic alliances?
- How can cybersecurity people play a more strategic role in their organization?
- What are good areas of professional development for security leaders to improve their communications?

Short Bio

- Has written lots (80+ articles for IBM-SI, 3xWP, 2xBooks) since 2015.
- Has worked with and for CIOs. Has shadowed CISOs. Has performed many cybersecurity gap analyses.
- Good communication is key to good management of cyber risks.
- Beyond academia, also consulting with
  - CISOs looking to improve their risk communications
  - Security vendors looking to improve their tools
  - Boards & executives looking to make sense of it all

Boards want to know…

Why are boards asking cyber questions?

Why are boards asking cyber questions?

- *Every board now knows its company will fall victim to a cyberattack, and even worse, that the board will need to clean up the mess and superintend the fallout.*

  See Ten Cybersecurity Concerns for Every Board of Directors

- *When you look at the bottom line, the monetary costs from the highly publicized Target breach are staggering: $150 million in initial response costs, $400 million in replacement credit cards, and an estimated $1 billion of ultimate costs.*

  See Directors Should Look Beyond Cyber Insurance: Law enforcement officials seek accountability in data breaches…

Why are boards asking cyber questions?

Board oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues.

— SEC Comm. Luis A. Aguilar, June 10, 2014

See Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus

Why are boards asking cyber questions?

Board oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues.

— SEC Comm. Luis A. Aguilar, June 10, 2014

See Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus

Why are boards asking cyber questions?

- Time-To-Lawsuits (TTL):
  - 9 days — 2011 Sony breach
  - Next-day — University of Central Florida (with a 2nd class action suit filed within 3 weeks) in early 2016
  - Same-day class action suit — Scottrade (2015).

See Nine Days from Sony Security Breach to Class Action

See 2nd class-action lawsuit filed versus UCF for data hack

See Scottrade announces data breach affecting 4.6M customers

Why are boards asking cyber questions?

- Because they're told by regulators and general counsel that they "have to" or "need to"
- Because class-action suits are waiting in the wind
- Because they see what can happen when shareholders go after them following a breach

- Because their jobs are on the line!

Top leadership needs help navigating

Are boards getting quality updates?

Board directors still not happy @ cyber

2015-2016 NACD Survey, 31% were dissatisfied or very dissatisfied with cybersecurity & IT risk information

32% of directors said their organization has “adequately tested cyber IR plans”

37% of directors said they get adequate reporting on cybersecurity metrics

Src: PwC’s 2017 Annual Corporate Directors Survey Report

What makes non-techies go huh???

What makes non-techies go huh???

Technobabble!

What makes non-techies go huh???

- Not speaking the language of the business
  - Are you a translator, a diplomat?
  - Can you speak in metaphors? Really, can you?
- Not using relevant indicators (KPIs) when reporting
  - Use metrics that all leadership can understand and rally around
- Not aligning any of the +/- risks with business objectives
  - Information risks only matter in the context of their impact on business objectives

What questions are boards/execs asking?

What questions are boards/execs asking?

According to KPMG, questions on directors' minds are:

- Am I asking the right questions?
- How do I get comfortable?
- Are we doing enough?
- How do I know we are doing the right things?
- Are we making the right decisions?

See KPMG: Connecting the dots: A proactive approach to cybersecurity oversight in the boardroom

What questions are boards/execs asking?

According to the NACD, here's what board directors are considering within their ranks:

- Do we understand the nature of the cyber threat?
- Do our board processes and structure support high-quality dialogue on cyber matters? (GRC/ERM)
- What are we doing to stay current as the cyber-threat landscape continues to evolve?

See Cyber-Risk Oversight: 3 Questions for Directors

Dynamics in the C-Suite

NIST's Viewpoint

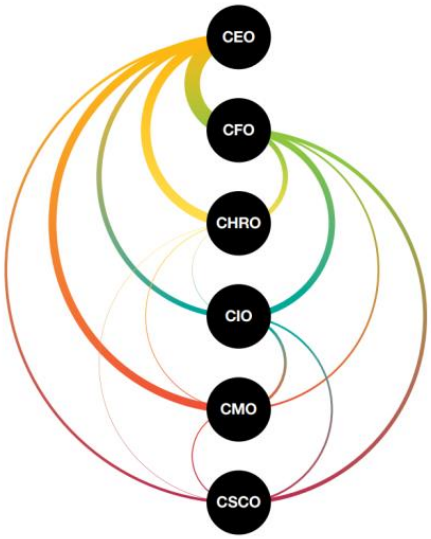
Cybersecurity is too important to be left to your IT department and operations groups. Cybersecurity must be a core issue for your corporate executive team. It can literally make or break your company.

— Dr. Willie E. May, acting director of NIST

See NIST speech, 4/17/2015: "Board Agenda: CYBER" Conference

Dynamics in the C-Suite

IBM asked each CXO which two colleagues they worked most closely with.



See IBM The Customer-Activated Enterprise (2013 study)

Dynamics in the C-Suite

- IBM's Securing the C-Suite report (2016) found:

  "the CFO, CHRO and CMO feel the least engaged in cybersecurity threat management activities, yet are the stewards of data most coveted by cybercriminals."

- When CXOs were asked about their level of engagement in cybersecurity preparations, CFOs reported the lowest level of engagement at 38%, followed next by CHROs at 41% and CMOs at 43%.

See Securing the C-Suite, Part 2: The Role of CFOs, CMOs and CHROs

Strategic alliances? Yes!

- Alliances make sense… CISOs weren't forged of the same metal as other CXOs.
- Alliances make sense… CISOs don't have decades of experience operating at CXO levels and reporting to boards.
- Alliances make sense… when it's not about being right, it's about communicating the +/- risks the best we can.
- Alliances make sense… at the top, that's how the game is played.

Cybersecurity is playing a more strategic role

We need to start acting like it

To play a more strategic role…

- Effective CISOs have leadership qualities on par with their CXO peers
- Cisco's Mitigating the Cybersecurity Skills Shortage report:
  CISOs must be able to frame the discussion in a strategic way that clearly communicates the potential impact of a data breach on stock price, customer loyalty, customer acquisition and the brand.
- IBM report: CISOs should be empowered "with the mission of managing information security risk across the enterprise and leading the initiative among the C-suite."

And that means good communication!!!

- The right focus
- The right interactions
- The right mindset
- The right communications (language, timing, framing)

Professional Development

Professional Development

Wisegate's CISO Handbook:

- Most important CISO skills (2013 survey): **Collaboration, Strategic Thinking and Influence**
- CISO: "I feel like we're part politician, part therapist, and part lawyer."
- CISO: "All leadership skills are important, but influencing without authority stands out."

See A CISO Handbook on Effective Leadership & the Art of Influencing People

Professional Development

Wisegate's CISO Handbook:

- Tip #1: Keep people informed with digestible updates
- Tip #2: Think like a negotiator
- Tip #3: Make their job easier
- Tip #4: Act in service to others

See A CISO Handbook on Effective Leadership & the Art of Influencing People

Cybersecurity 2.0 skills

- Translator — Are you communicating in language appropriate for your audience? Clearly, effectively, in the language of the business, through explanations, metaphors or visual aides.
- Diplomat — How's your EQ? When you speak, are people open or closed to your suggestions? Can you negotiate?
- Strategic thinker —business acumen, include the big picture in all decisions, and connect the dots about the risk implications of all decisions.

Leadership Qualities

Executive search and leadership consulting firm Spencer Stuart looks at:

- Exceptional business judgment;
- The ability to recognize interpersonal dynamics and apply them in decision-making;
- Highly effective people management and team building skills;
- Humility and substance;
- Effective people development skills;
- The ability to drive change.

Leadership Qualities

- Egon Zehnder, professional services firm:

  the CISO is expected to act as a full strategic partner with the rest of the C-suite

- Look at
  - *Results orientation*
  - *Strategic orientation*
  - *Transformational leadership*
  - *Relationship management*
  - *Team leadership*
- List 4 elements of potential

  Curiosity | Insight | Engagement | Determination

See Evaluating and Attracting Your Next CISO: More Sophisticated Approaches For a More Sophisticated Role

Effective CISOs continually seek to grow their perspective & influence beyond the confines of IT.

CISO Leadership Qualities

Four faces of the CISO's role according to Deloitte's CISO Transition Lab workshops:

1. **Strategist**: drive business and cyber risk strategy alignment and instigate transformational change to manage risk.
2. **Adviser**: CISOs educate, advise and influence activities with cyber risk implications.
3. Guardian: Leaders protect business assets by managing the effectiveness of the cyber risk program.
4. Technologist: Assess and implement security technologies and standards to build organizational capabilities.

Taking it all in

Boards are increasingly likely to question the organization's management of cybersecurity issues

And that's a good thing…

Now let's meet those expectations!

In their own words

Ultimately, the goal of sharing metrics is to make sure there's a follow-up discussion with the higher-ups to make an informed decision.

— Prasanna Ramakrishnan, VP of IT Risk Management at Career Education Corporation

See Tenable - Using Security Metrics to Drive Action

In their own words

We need to agree on the metrics that make the most sense to everybody across the entire C suite. It's not just the chief executive officer: it's the head of finance, the head of marketing , the head of human resources.

— Andrew Storms, VP of Security Services at New Context

See Tenable - Using Security Metrics to Drive Action

In their own words

Everything that gets presented to the board has to have a clear link back to business value and business strategy.

— Aaron Weller, Managing Director, Cybersecurity & Privacy at pwc

See Tenable - Using Security Metrics to Drive Action

Audience Focused Communications

Keep in mind

- Focus (business)
- Granularity
- Information
- Terminology
- Timing
- Tone

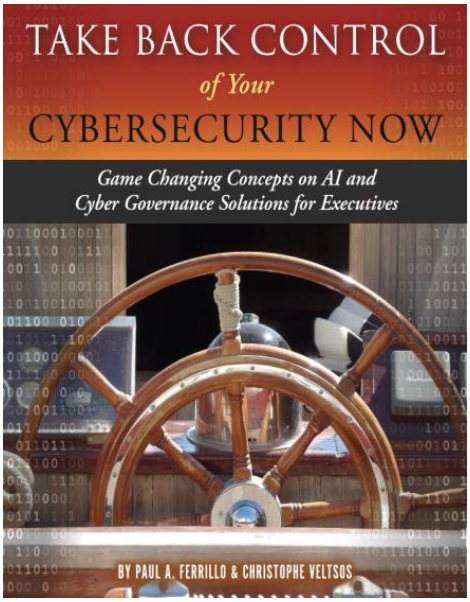
TGIF Mnemonic (T3GIF)

- (T) Timing
- (T) Tone
- (T) Terminology
- (G) Granularity
- (I) Information
- (F) Focus (business)

Resources

Resources

- Co-authored a book with Paul Ferrillo, a data-breach lawyer from NYC.
- Available in PDF for free
- Available on Amazon in Kindle & paperback formats
- Cybersecurity for executives



Resources

- Audio/Book: HBR's 10 Must Reads on Communication
- Book: World Class Risk Management (N. Marks)
- Book: The Trusted Advisor
- Book: Rhetoric, Logic, & Argumentation
- Article: Forrester's The CISO's Handbook — Presenting To The Board ($)
- Books on boards & governance (or management and leadership)
- And all the links found throughout the presentation

Additional Resources

Cyber Risk Communications – (MSU IT653 – Summer 2018)

- 100% online course, meets twice a week (May/June) for ~70 minutes, 3 grad credits
- Focused on how we can improve the way we communicate about cyber risks.

Content: analyze audience; define report outline and objectives for target audience (IT, executives, audit & compliance); ethos/pathos/logos concepts; white papers. Data misrepresentations, intentional or unintentional; appropriate use of data visualization tools and dashboards; representing needle in haystack data (low volume, high risk).

Thanks for the

Let's talk. Over coffee?

- Email: chris@drinfosec.com
- Twitter: @DrInfosec
- LinkedIn