CYBER SECURITY SUMMIT 2016

Finding Cyber Gems

And steering clear of potential cybersecurity or privacy landmines

Chris Veltsos, aka Dr.InfoSec

Agenda

- Overview of key cybersecurity growth areas: cybersecurity technology, enabling more strategic decisions, and employees
- How can cybersecurity and privacy issues impact your investments?
- How can I get help with these issues?

Long Bio

Dr. Christophe Veltsos - Handbill

Cyber Risk Strategist | Digital Trust Advisor
Cybersecurity Speaker

Chris – aka Dr.InfoSec – is passionate about helping organizations take stock of their cyber risks and manage those risks across the intricate landscape of technology, business, and people. Whether performing information security risk assessments,
working alongside CIOs & CISOs to set and communicate strategic cybersecurity priorities, or advising board directors on effective governance of cyber risks, Chris enjoys working with business leaders to improve their organization's cyber risk posture.

Since 2008, Chris has presented at the local, regional, and national level, including at major security conferences like RSA & CSI DC. Chris has written articles, book chapters, and blog posts about cybersecurity and privacy.

Both faculty and practitioner, Chris maintains the DrInfoSec.com blog, tweets as @DrInfoSec, and writes articles about cyber risks for IBM's SecurityIntelligence blog. Connect with Chris on LinkedIn.

Key Skills & Accomplishments

- Knows the value of clear communication, managing human assets and relationships, managing risks.
- Has worked with and for CIOs. Has shadowed CISOs.
- Has performed cybersecurity gap analyses for over ten clients.
- Has delivered over ten information security roadmaps to clients.
- Has authored a ten-page white paper for an information security consulting business. The white paper received very positive feedback from CISOs.
- Has authored over 30 articles about cyber risks, CISOs, and the value of strong communications in the boardroom and the C-Suite for IBM's Security Intelligence blog.
- Is recognized for his expertise and his writings: DrInfoSec blog listed on on *Top 50 InfoSec Blogs You Should Be Reading* (by Digital Guardians); also named in *Top 50+ Tech Influencers and Thought Leaders* (by DNSstuff.com); one article listed in *The 20 Most Influential IT Management Posts of 2015* (by CapTerra).
- Veteran speaker, including as featured speaker and keynote speaker.
- Is an academically and professionally qualified (CISSP | CISA | CIPP) cybersecurity consultant & educator.

Professional Activities

2015-present	*Contributing Author*, IBM Security Intelligence blog. Authored over 30 articles on cyber risks, board and CXOs, CISOs, and the value of strong communications in the boardroom and the C-Suite.
2007-present	*Cybersecurity Risk Analyst*, AdvanceIT Minnesota. Performed information security and risk assessments for more than 10 public and private organizations.
2012-2014	*Subject Matter Expert*, Walden University. Curriculum development of two new graduate-level Information Security courses for a leading higher-education online institution.
2010	*Technical Editor, Securing the Smart Grid: Next Generation Power Grid Security* (Syngress).
2008	*Co-Editor*, SANS.org NewsBites. Edited semi-weekly newsletter about information security.
2007-2009	*President*, Mankato Chapter of the Information Systems Security Association (ISSA).

Short Bio

- Faculty member, teaching in IT for 18 years, teaching in security for over 10 years.
- Outside the classroom, consulting for over a decade.
- Has worked with and for CIOs/CEOs. Has shadowed CISOs.
- Has performed many cybersecurity gap analyses.

- Ready to help you quickly triage through the cybersecurity issues of your investments.

For success, your business needs…

- **Sales** are a key business function…
  Sales are a function key to your business…
- **Accounting** is a key business function…
  Accounting is a function key to your business…
- **Security** is a key business function…
  Security is a function key to your business…

CEOs worry about cybersecurity

PwC's 18th Annual Global CEO Survey (2015):

- 61% of CEOs are concerned about "cyber threats, including lack of data security."
- 53% of CEOs reported cybersecurity as being very important strategically.
- Of strategic importance:
  1. Mobile technologies for customer engagement at 81%
  2. Data mining and analysis at 80%
  3. Cybersecurity at 78%

One person's worry is another person's opportunity

Cybersecurity Investment Areas

1. AI & machine learning.
2. Improving the quality of information used to make cybersecurity decisions (cyber risk quantification and maturity-based approaches to cyber-risk reporting/ planning).
3. Helping organizations leverage their employees as human sensors, from better metrics on the effectiveness of security awareness programs, to more timely, more engaging, more effective security awareness activities (i.e. security culture).

Opportunities

- Go for automation
- SOAP – Security Orchestration & Automation => Profit
- Go for machine learning & artificial intelligence
- Go for investing in what will help humans (employees)
- Go for investing in what will help decision-makers

Axiom:
Cyber can be the greatest disruptor of value for your investments

If you don't do regular check-ups, you could find yourself with an emergency situation.

NIST's Acting Director

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 Dir. of NIST

Src: NIST.gov: "Board Agenda: CYBER" Conference

Common Misery?

- Anthem
- eBay
- OPM
- Sony Pictures
- Target
- Yahoo

Which one of these entities didn't have dedicated staff for information security?

Lawsuits…

- 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 (past year).

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

What kind of data do you have?

- Nature of your customers/clients
- Number of records kept
- Highly sensitive data or intellectual property?
- Potential target? (military contracts, medical records, key parts manufacturer, Hacktivists, easy prey)

Ignoring this won't make it go away

- Optimism bias: "*a cognitive bias that causes a person to believe that they are less at risk of experiencing a negative event compared to others.*"
- Four factors of optimism bias:
  - their desired end state,
  - their cognitive mechanisms,
  - the information they have about themselves vs others,
  - and overall mood.

Src: https://en.wikipedia.org/wiki/Optimism_bias

Simple security truths

- You can never be 100% secure
- Small business:
  Security is about helping the business stay in business
- Medium/Large business:
  Security is about helping the business achieve (or not miss) its objectives

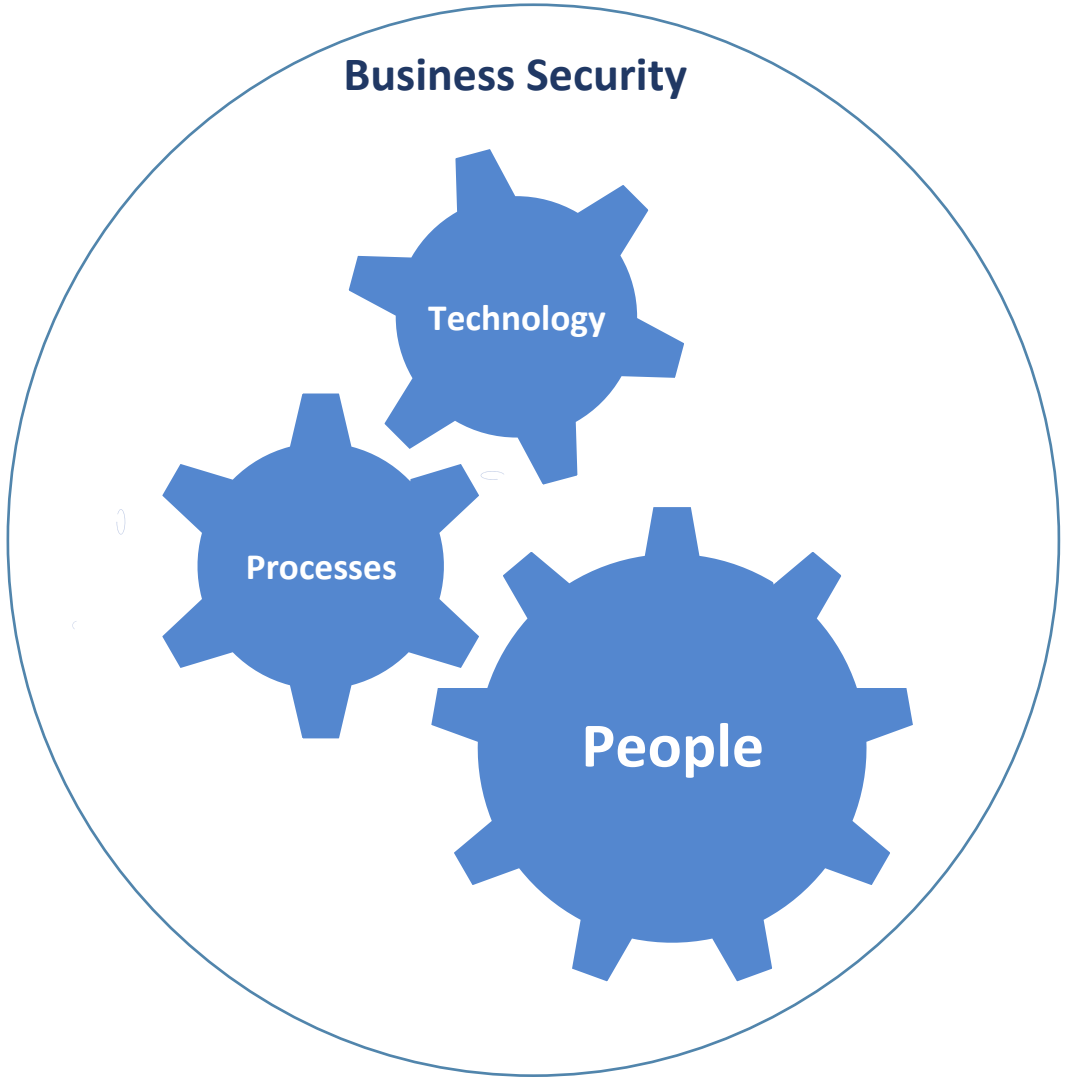
Before signing the deal

Perform a quick assessment of CURRENT cybersecurity and privacy issues & future outlook

Even simple things can tell you a lot about the state of things…

Review People, Processes, & Technology

- Look at the PPT of Security
- Review each area in depth
- Is each area aligned in support of the business?
- Is each area used effectively?



Considering hiring a security person?

- The right background/experience
- The right focus
- The right mindset
- The right interactions
- The right communications

Considering hiring a security consultant?

- Pick someone willing to
  - Learn about your business
  - Learn about what's important to you and your business
  - Help YOU make decisions about the best course of action
- Like a good doctor…
  - Listens to the symptoms you describe
  - Learns about your likes and dislikes
  - Make a decision together
  - Follow-up appointment to check on things

Questions to consider

1. Does the business know its security risks? Its privacy risks?
2. Do we have a good understanding of how these risks impact the value of our investment today? In the future?
3. What can be done to effectively remediate unacceptable risks? What will be the cost & effort required to do so?
4. What can we do to ensure cyber risks are effectively taken into account, and clearly & frequently communicated?

Let's talk. Over coffee?

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