CYBER SECURITY SUMMIT 2016

Cybersecurity — Seven Ways to Keep Your Small Business Running in the Era of Viruses, Scams, and Breaches

Chris Veltsos, aka Dr.InfoSec

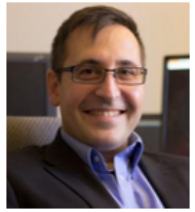
Agenda

- Asking questions is how we learn & improve
- Why should you care about security?
- Why is your business a target? What threats?
- What's the magic solution?
- Where do I start? Where do I go next?
- What are some key principles? What does it mean in plain English?
- What if I need more help?

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.

- Working to assist SMBs with their security needs.

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…

#1 Ask questions on how cyber can impact your business

Here, today, next week, next month.
Don't wait too long.

#2 Understand why you need to care about security

Pressures & drivers

- Federal & state regulations
- PCI compliance & what it doesn't cover
- Third Party vendor agreements & pressures
- Cyber insurance

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

#3 Understand why you might be a target & what the threats are

Who you are as a business matters a lot

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

Main Threats to SMBs

- Ransomware
- Frauds & scams
- Focused hackers, hacktivists
- Threats from within ("insider threat")
  - Mistakes
  - Malicious
  - Manipulated

104 Ransomware Variants (as of Oct 2016)

Src: http://www.cyber.nj.gov/threat-profiles/ransomware/

777	7ev3n	Alfa	Alma Locker
Alpha	Alpha Crypt	AnonPop	Apocalypse
AutoLocky	BadBlock	Bandarchor	Bart
BitStak	Black Shades	Bucbi	CTB-Faker
CTB-Locker	Central Security Treatment Organization	Cerber	Chimera
CoinVault	Coverton	CryPy	CrypBoss
CrypMIC	Crypren	CryptFile2	CryptMix
CryptXXX	CryptoBit	CryptoHost	CryptoJoker
CryptoRoger	CryptoWall	Crysis	DMA Locker
DXXD	DecryptorMax	Ded Cryptor	DetoxCrypto
Dogspectus	Domino	EduCrypt	El Gato
FBI MoneyPak	FLocker	FSociety	Fantom
GPCode	Globe	HDDCryptor	Hidden Tear
Hitler-Ransomware	HolyCrypt	Jigsaw	JuicyLemon
KimcilWare	Koler	KozyJozy	Linux.Encoder
LockLock	Lockdroid.E	LockerPIN	Locky
MIRCOP	MM Locker	MSIL/Samas.A/ Samsam	Maktub Locker
MarsJoke	NanoLocker	Nemucod	NoobCrypt
PadCrypt	Petya	PizzaCrypts	PokemonGo Ransomware
Power Worm	PowerWare	R980	RAA
Radamant	Ransom32	RektLocker	Rokku
SNSLocker	Satana	Shark	Simple_Encoder
Simplelocker	Smrss32	Stampado	TeslaCrypt
TorrentLocker	TowerWeb	Troldesh	TrueCrypter
Unlock92	VirLock	Wildfire	XRTN
Xorist	ZCryptor	Zimbra	cuteRansomware

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

#4 Understand there are no magic solutions

If it's too good to be true…

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

Where do you start?

Good news: there are many resources for you to use

#5 Start somewhere on the road to better security

Start by reviewing & adapting existing security resources

Physical security

Yes, it does matter!

BBB's 5 Steps to Better Business Security

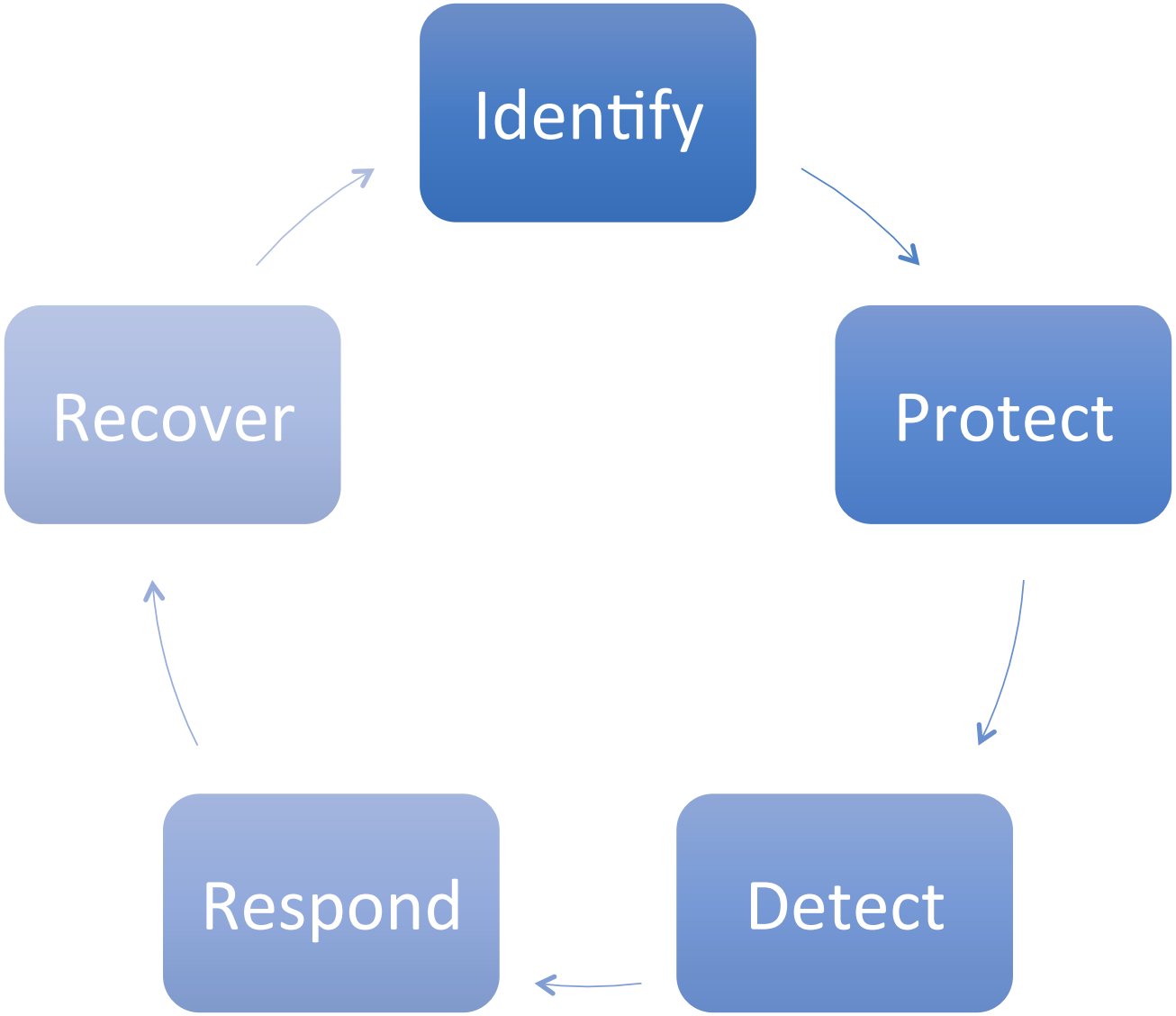
- Identify
- Protect
- Detect
- Respond
- Recover

see https://www.bbb.org/council/for-businesses/cybersecurity/the-5-step-approach/

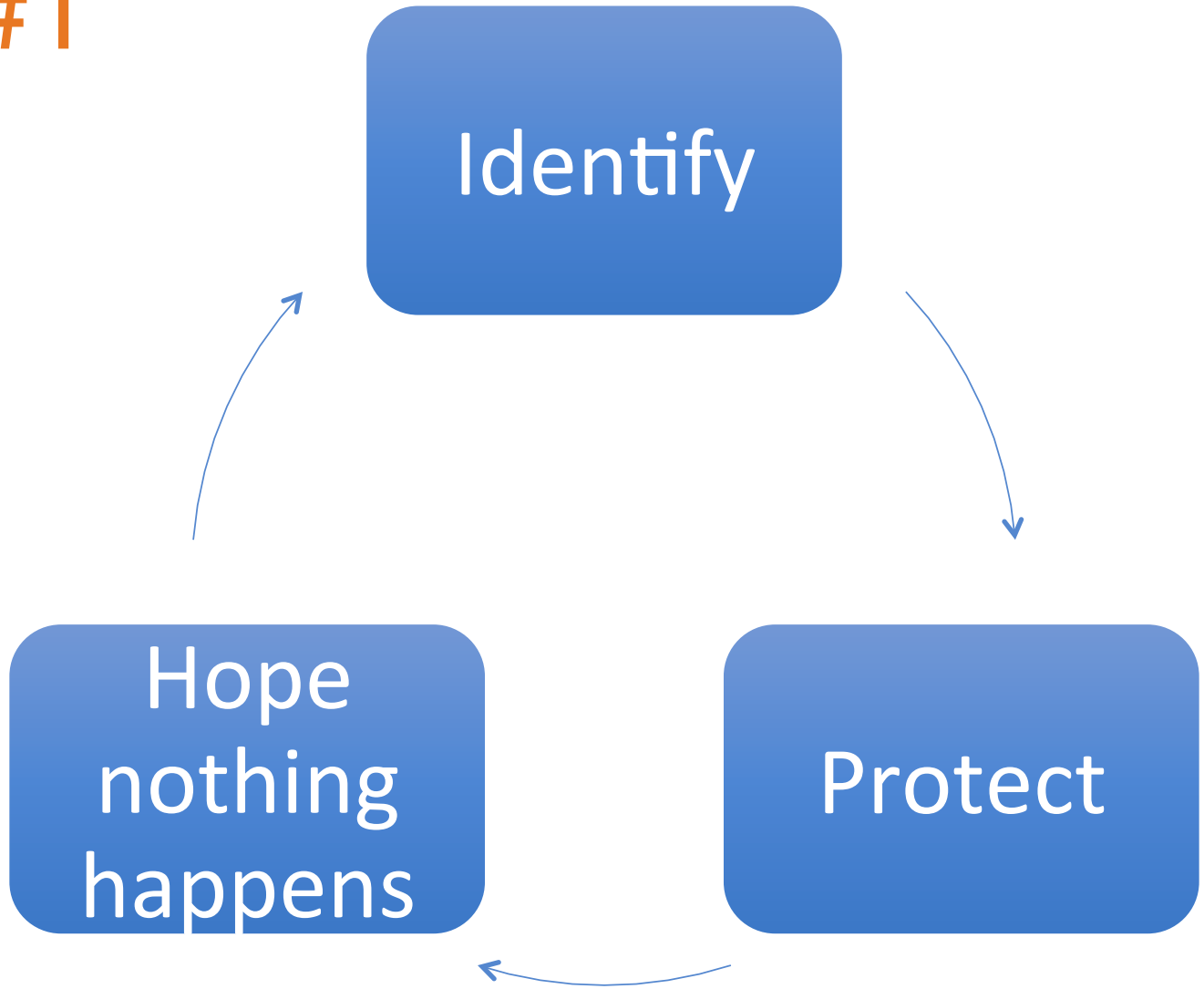
BBB's 5 Steps to Better Business Security

see https://www.bbb.org/council/for-businesses/cybersecurity/the-5-step-approach/

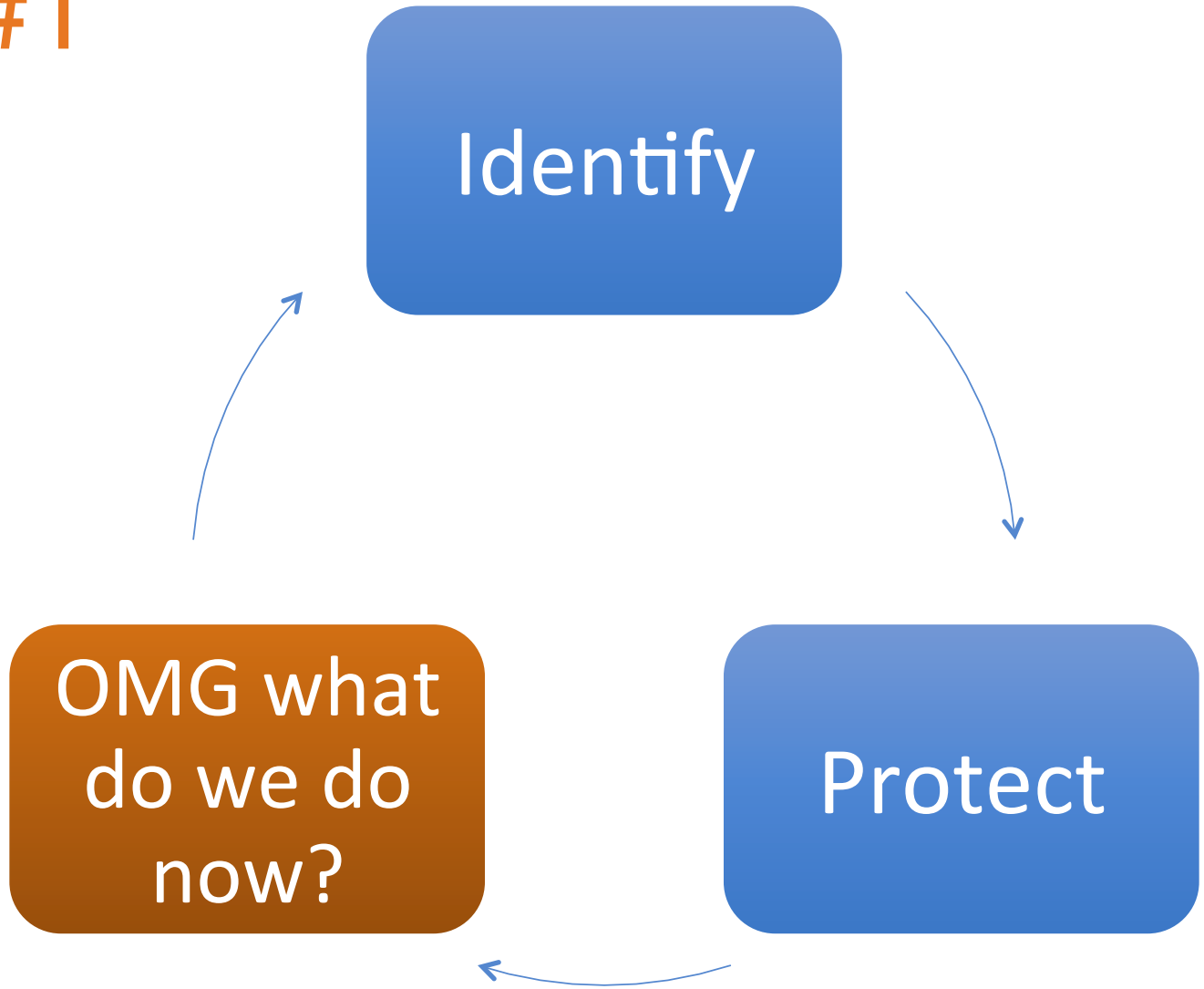
Theory



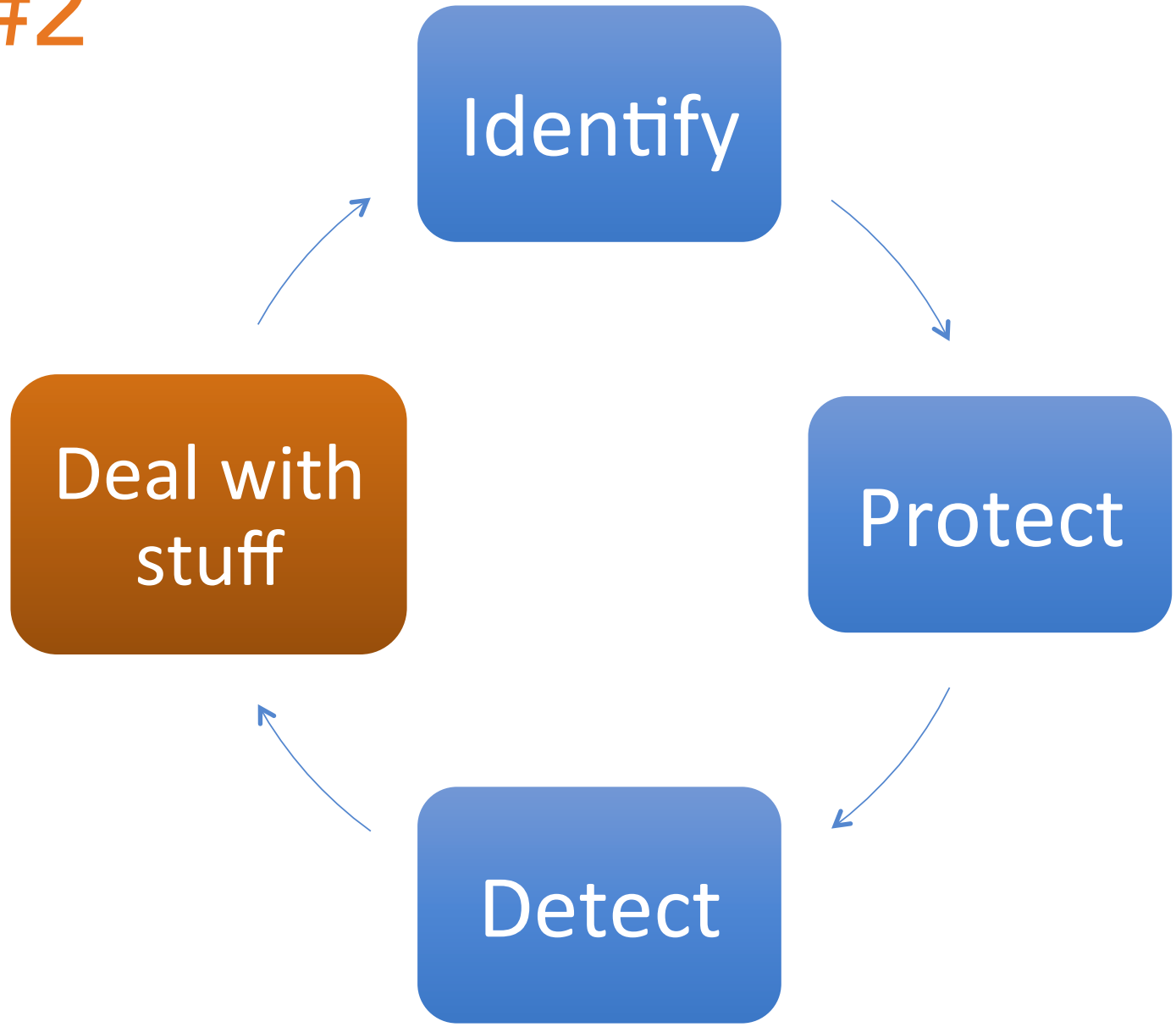
Reality #1



Reality #1

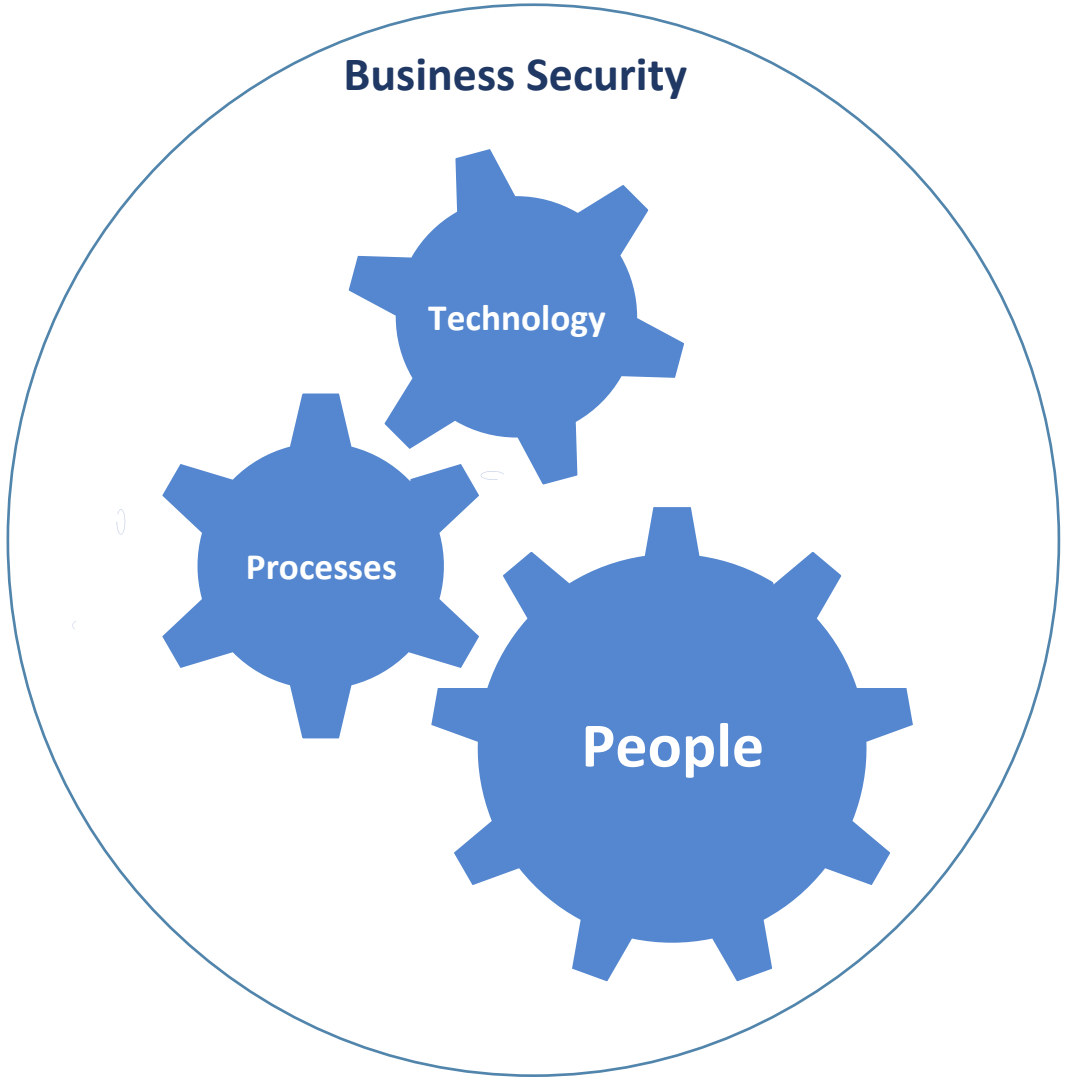


Reality #2



Leverage People, Processes, & Technology

- Use all three, the PPT of Security
- Some solutions will be cheaper than others
  - E.g. implementing policy/ process is often cheaper than technology



Involve key allies on your staff

- Engage your financial/business leadership
- Engage your HR leadership
- Engage your IT leadership
- Educate & train your entire staff to be your eyes & ears

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%

Involve all employees

- Security is a all-hands-on-deck activity
- Educate & train your entire staff to be your eyes & ears
  - Work to create "human sensors"

#6 Some Key Security Principles

Key Security Principles – 1-10 staff

1. Review your overall information security hygiene
   use up-to-date antivirus, patch operating systems, and regularly update all software
2. Do not rely on default credentials or default settings
3. Back up important data & ensure the backup system works
4. Stay current on cyber security issues & educate your employees

Key Security Principles – 1-10 staff

1. Review your overall information security hygiene
2. Do not rely on default credentials or default settings
3. Back up important data & ensure the backup system works
4. Stay current on cyber security issues & educate your employees

1. How do we keep our systems safe?
2. How can we prevent easy access to sensitive data?
3. How can we restore data/ systems after an incident?
4. What are we doing to stay current & how are we informing our employees?

Key Security Principles – 10-50 staff

1. Classify data to help you protect what matters most
2. Review your data lifecycle
3. Ensure proper disposal of documents and devices containing sensitive data
4. Establish strong controls around key financial areas of your business

Key Security Principles – 10-50 staff

1. Classify data to help you protect what matters most
2. Review your data lifecycle
3. Ensure proper disposal of documents and devices containing sensitive data
4. Establish strong controls around key financial areas of your business

1. What different types of data do we have? How sensitive is that data?
2. What data do we collect? How long do we keep it?
3. Are we properly disposing of data we no longer need?
4. How are we protecting our financial assets?

Key Security Principles – over 50 employees

1. Take security awareness seriously
2. Keep systems patched
3. Segment your network
4. Consider adopting a comprehensive security solution (a UTM dashboard)

Key Security Principles – over 50 employees

1. Take security awareness seriously
2. Keep systems patched
3. Segment your network
4. Consider adopting a comprehensive security solution (a UTM dashboard)

1. How do we help our employees stay safe?
2. How can we keep systems protected?
3. How can we keep our networks safe?
4. How can we leverage tools to give us better alerts and visibility?

#7 Find a trusted guide to help you along the way

Security folks sound weird

- Too often, security is full of technobabble!
- Don't let that scare you.
- Find the right person for you and your business… someone who can help translate how security things impact your business.

Considering hiring a security person?

- The right focus
- The right interactions
- The right mindset
- 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

Short recap

- Security doesn't have to be scary.
- Start somewhere, and keep at it.
- Make incremental progress.
- Double-check things.
- Ask for help before something happens.

Short recap

- Security doesn't have to be scary.
- Start somewhere, and keep at it.
- Make incremental progress.
- Double-check things.
- Ask for help BEFORE something happens.

Let's talk. Over coffee?

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