RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: CXO-F01

Cybersecurity: You're Doing IT Wrong

Jared Carstensen

Chief Information Security Officer (CISO), CRH Plc
@jaredcarstensen

Introduction – My Journey

Every kid has dream jobs growing up……

Baby

Firefighter

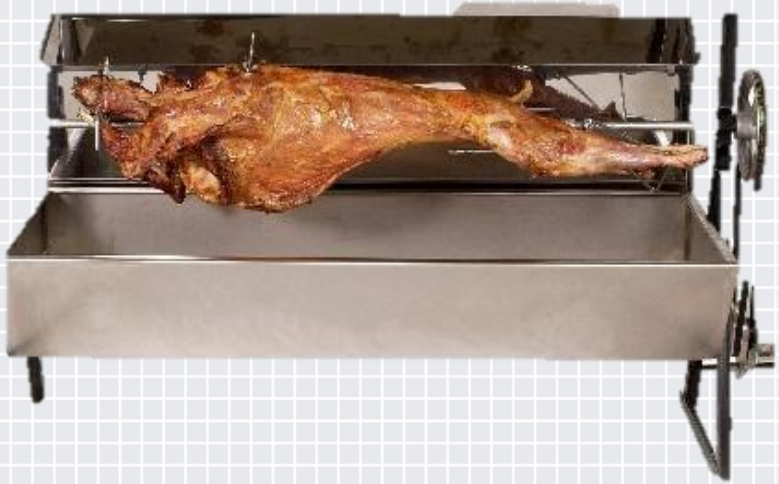
Policeman

Leader / Politician

CISO

Perceptions vs. Reality – Before & After

Before Breach

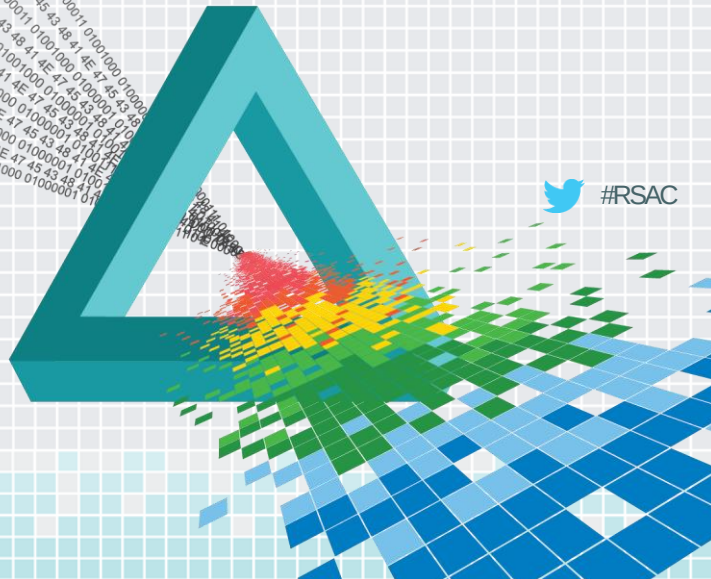


During & Post Breach

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Why Are We Doing IT Wrong?



#RSAC

Keeping it Simple!

- All of it — everything, make it secure!
- Applications — apps and more apps
- Awareness — constant challenge
- Audit — multiple synergies & often ‘forgotten’

Keeping it Simple!

- Business vs. security – purpose and function
- ‘Burning bridges’ & long term strategy – working with people
- Bring Your Own Device (BYOD) & Bring Your Own Cloud (BYOC) = bring your own problems & increase risks

Keeping it Simple!

- Context — all about risk!
- Communication — we stink at it!
- ‘Consumerization’ — who are the biggest challenges / risks?
- Cloud Computing — what is going on?
- Compliance — we don’t engage enough!

Keeping it Simple!

- Data — we apply security wrong! boxes vs. assets
- Disruptive — we tend to approach things in the wrong way
- Dissecting — what is needed vs. what matters?
- Develop — cybersecurity aware culture & workforce

Keeping it Simple!

- Endorsement — why we do what we do?
- Engagement — who should we be working with?
- Efficiency — duplication everywhere!
- Environmental / situational awareness — knowing the business
- Evolving — from ‘no’ to ‘let’s work together’

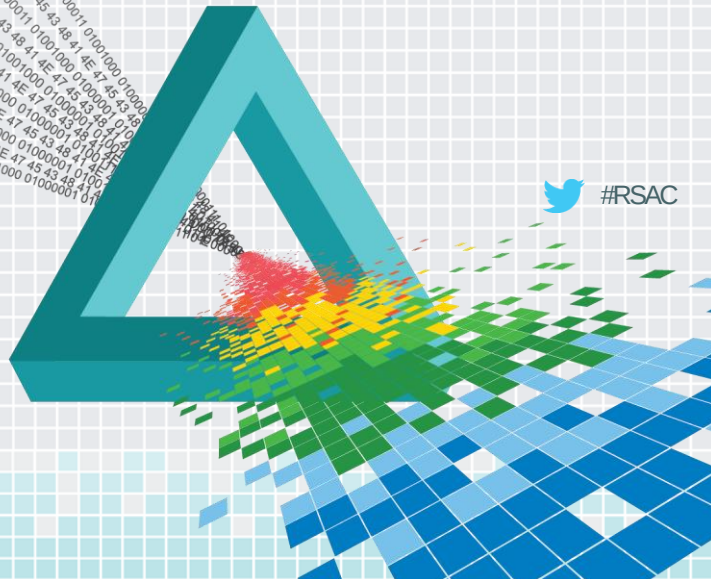
Keeping it Simple!

- Finding the ‘champions’ — who supports our objectives?
- Failure to manage expectations — security cannot prevent all attacks and breaches!
- Fetching quick wins — not everything needs a major project!
- Fashion industry — rate of change & trends!

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Applying Effective Security - A to Z



Getting it Right – Applying in Reality!

- Awareness is often the best return on investment
- Business enablement and engagement will define your success
- Culture can make or break security efforts – find out what ‘has worked’ vs. ‘has not’
- Do not try do it all! Prioritize, plan & deliver
- Engage with sponsors & be the solution – not the ‘no’ or barrier!
- Focus on what really matters – people will forget non-essentials
- Give options & practical solutions
- Help others achieve their goals & objectives
- Inform, interact and involve others in the decision process
- Justify your role and the need for security
- Know your strengths & weaknesses – play to strengths, build around weaknesses

Getting it Right – Applying in Reality! (cont)

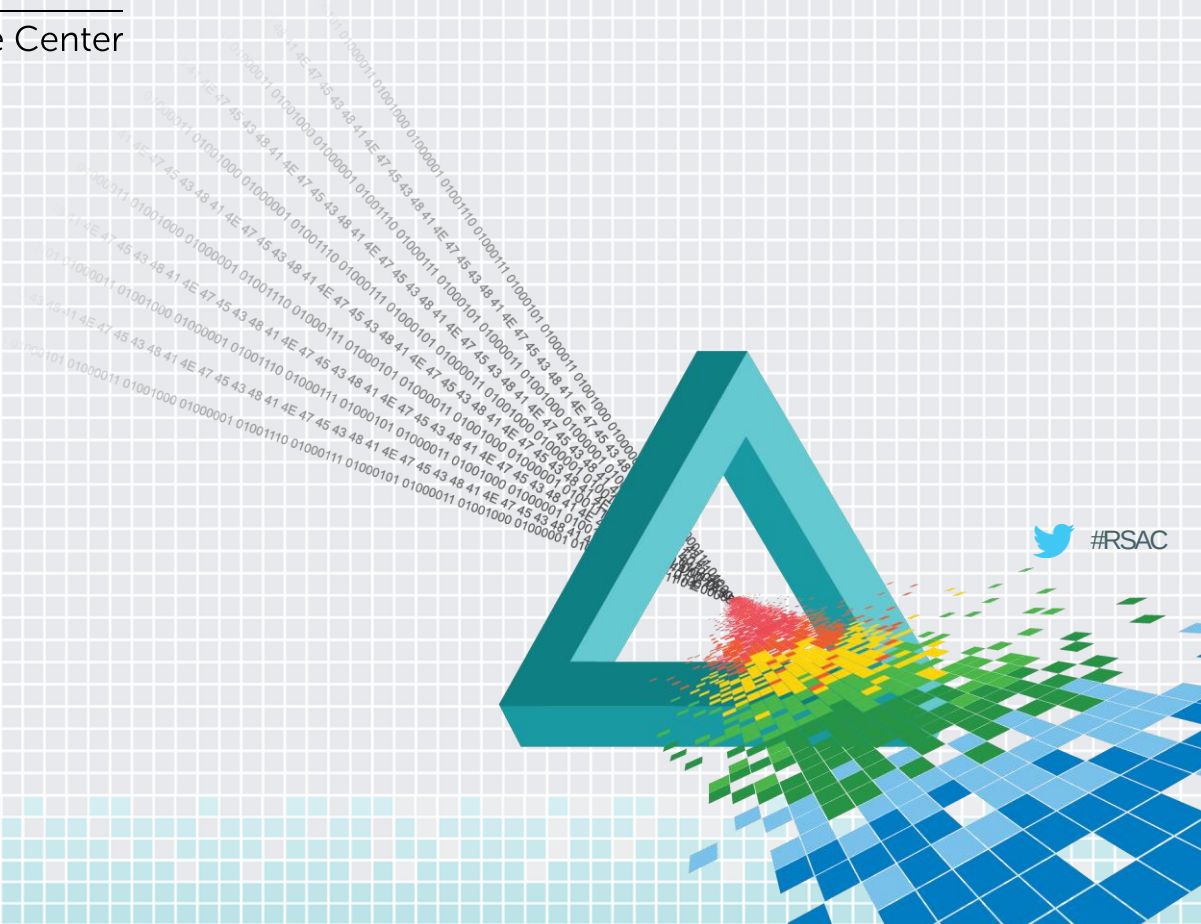
- Learn from other mistakes & real world events
- Manage expectations – you cannot stop every attack
- New technologies do not necessarily fix age old problems
- Outline key objectives, challenges and requirements to stakeholders
- Provide metrics – if it cannot be measured, it cannot be managed
- Question yourself and how things are currently being done (understand, not challenge)
- Response capabilities may well save your company and your career – response never goes out of style
- So what? Ask yourself what will happen if we do, and what will happen if we don't
- Technology is one component, people and processes will always be the front and center for security
- Validate ideas and approaches internally prior to executing

Getting it Right – Applying in Reality! (cont 2)

- What is the worst thing you could say to your stakeholders at 3AM? This will help understand what matters most to them and what you will need to focus on
- XaaS – can you deliver the same value to the business using different models or approaches?
- Yesterday's threats and attacks are still the big headache
- Zero in on the things that matter most to your business stakeholders

Reality Check: Our mission and objective should be to enable more secure and resilient services, while protecting our organization's brand, it's customers and employees. We will never stop all attacks, but our success should be determined by our ability to respond and 'stop the bleeding', while continuing to deliver services to customers and users.

Sanity Check



In Summary & Final Thoughts!

Car Accidents vs. Security Breaches

- Rules of road to protect drivers and pedestrians
- Regulations and standards to protect businesses and consumers
- Speed limits depending on the type of road
- Regulations depending on the type of industry and sector
- Wide choice of cars available depending on your needs
- Wide choice of solutions and providers depending on your requirements
- By not adhering to rules and laws of the road, you put your own and others' lives at risk
- By not adhering to security rules, standards, frameworks and best practice, thousands of incidents are happening every days putting your organization and its customers at risk
- Despite all road safety guidelines, laws and awareness there are countless road accidents and fatalities every day
- Despite all the standards, guidance, frameworks, regulations and more solutions and services than ever before; countless incidents, breaches and non-compliance continue

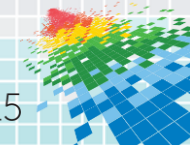
Is your organization driving recklessly, or are they simply asleep at the wheel?

Thank You!

"If you talk to a man in a language he understands, that goes to his head. If you talk to him in his language, that goes to his heart."

~ Nelson Mandela

Jared Carstensen

Chief Information Security Officer, CRH Plc

@jaredcarstensen / LinkedIn / etc.