Cybersecurity
Getting the Business Engaged

ALLAN BOARDMAN
CYBERADVISOR.LONDON

20 SEPTEMBER 2017

About the Presenter

Allan Boardman CISA, CISM, CGEIT, CRISC, CA(SA), ACA, CISSP

- Most recently Business Information Security Officer – GSK London
- Background in Audit, Risk, Security and Governance roles
- Chair ISACA International Audit and Risk Committee, 2014/15 – currently a member
- Chair ISACA International Credentialing Board & Career Management Board, 2011/14
- Member ISACA International Board of Directors, 2011/14
- Member ISACA International Strategy Advisory Council, 2011/14
- ISACA International Vice President, 2012/14
- Member ITGI Board of Trustees, 2012/14
- Chair CISM Certification Committee 2009/11, member since 2006
- Member ISACA CGEIT Certification Committee 2016/17
- Member ISACA Leadership Development Committee 2010/11
- London Chapter President 2004/06. Chapter Board member 1999/08
- Paralympics and Olympics Volunteer – London 2012, Sochi 2014, Rio 2016

Setting the scene

Full business engagement is essential to provide appropriate and sufficient protection to business most critical IT and information assets.

This session will share a practical approach to ensure that the business is fully engaged in cybersecurity efforts.

What is the main problem?

- □ CIO is accountable for cybersecurity
- □ Business still thinks IT is responsible for managing cybersecurity
- □ Cybersecurity not integrated into Enterprise Risk Management (ERM)

Challenges Facing Information Security

- ❑ Information security is continually moving up board agendas
- ❑ Information security professionals find it challenging to help business leaders understand the cyber risks across increasingly digital businesses
- ❑ The challenge is not necessarily that the business failing to grasp cyber risk
- ❑ But addressing the communications gap between technical staff and business management

What Typically Happens in Practice

- Organizations have many of the pieces and parts to a security program (policies, standards, firewalls, security team, IDS, etc.)
- These pieces and parts are the responsibility of a small security team that is charged with making sure that security happens.
- Security must be implemented throughout the organization, and having several points of responsibility and accountability is critical.

- But the management is not truly involved, and security has not permeated throughout the organization.
- If security was just a technology issue, then this security team could properly install, configure and maintain the products.
- Coherent system of integrated security components that exist to ensure that the organization survives and thrives.

Security incident: Who worries about what?

Business leaders: Business Risk

- ❑ How bad is it?
- ❑ Who was it?
- ❑ How did they get in?
- ❑ What information was taken?
- ❑ What are the legal implications?
- ❑ Is it under control?
- ❑ What are the damages?
- ❑ What do we tell people?

Security team: Security Detail

- ❑ Account lockouts
- ❑ Failed user access attempts
- ❑ Web shell deletions
- ❑ Buffer overflows
- ❑ SQL injections
- ❑ Cross-site scripting
- ❑ Denial-of-service
- ❑ IDS/IPS events
- ❑ Incident level fixes

What the business wants

- ❑ Full visibility
- ❑ Rapid insight
- ❑ Business context
- ❑ Efficient and comprehensive response
- ❑ Aligned to business priorities
- ❑ Risk managed from business perspective
- ❑ Business driven security linking

Business driven security strategy

- ❑ Prioritize assets and understand their vulnerabilities
- ❑ Quantify business risk and impact if those assets were compromised
- ❑ Build a strategy to defend those assets with clear cost/benefit
- ❑ Ensure strategy is holistic (people, process, technology)
- ❑ Determine gaps between what you have in place and your ideal state
- ❑ Take a phased approach to addressing the gaps
- ❑ Prioritize according to impact on risk posture
- ❑ Constantly re-evaluate threats and vulnerabilities to tune your strategy
- ❑ Have a response plan in place

Risk Convergence

- ❑ The business relies on technology like never before
- ❑ Business and digital strategies are intertwined
- ❑ Information and technology risks are board level topics

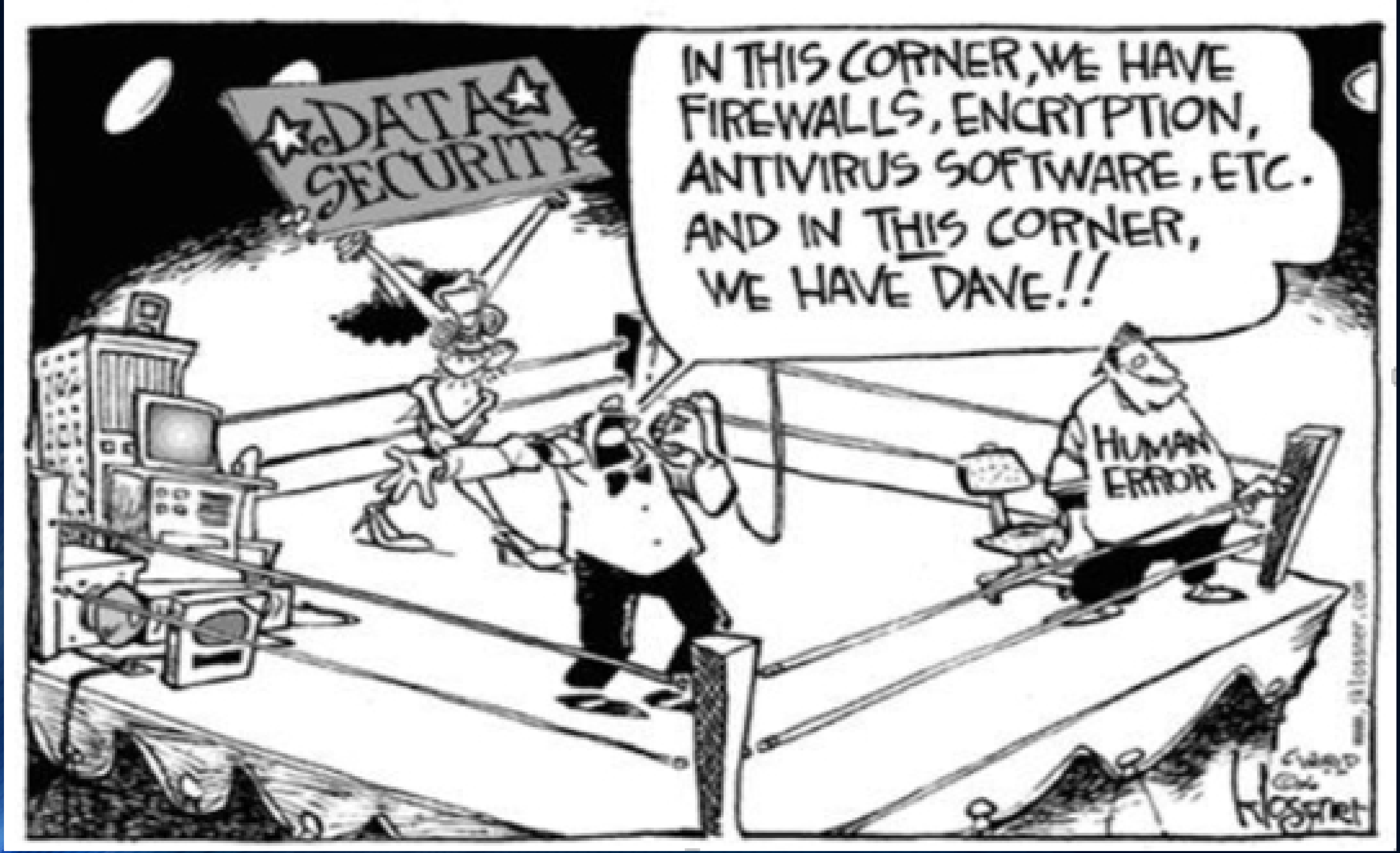
To be successful in today’s market, organizations must address cyber risk and business risk together

Cyber Risk as an Enterprise Risk

- ❑ Cyber-risk is a business risk that must be managed within an overall information and risk management framework.
- ❑ Crucial to demonstrate that cyber risk is another business risk to be considered across the spectrum of other key business activities and managed like other business risks.

The Human Factor

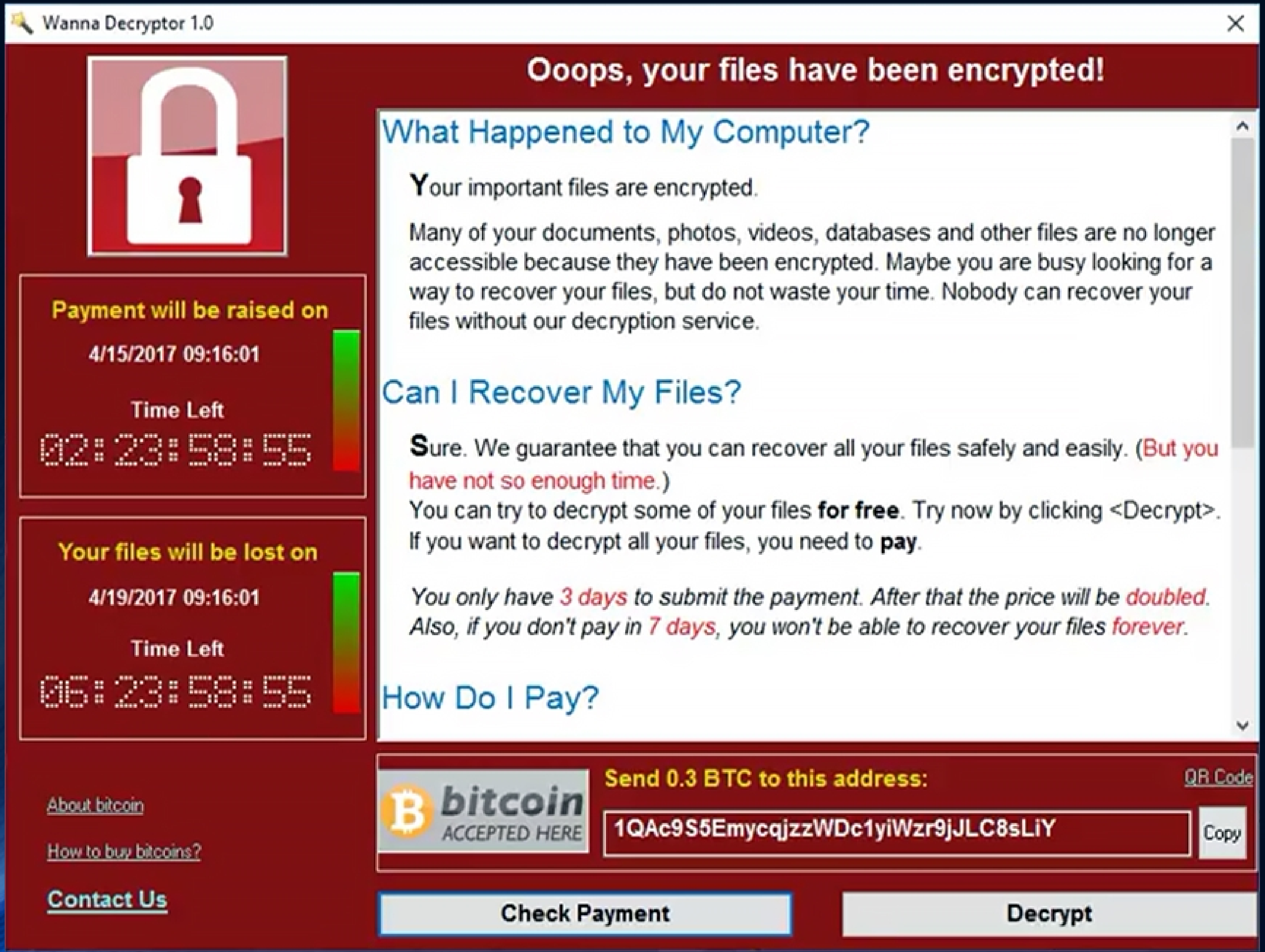
You still have to think about Dave!!!!



DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

So exactly how do we engage?

Does this engage the business?



Ooops, your files have been encrypted!

Payment will be raised on

4/15/2017 09:16:01

Time Left

02:23:58:55

Your files will be lost on

4/19/2017 09:16:01

Time Left

06:23:58:55

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Send 0.3 BTC to this address:

1QAc9S5EmycqjzzWDc1yiWzr9jJLC8sLiY

Structured Approach to Business Engagement

Threat and Risk Workshop approach to proactively identify, track and address threats.

- □ Identify most critical information assets
- □ Identify threats and attack scenarios that target these assets
- □ Determine required protection required
- □ Identify current controls
- □ Identify current risk exposure
- □ Agee action plan for addressing gaps

In Summary

- ❑ The Executive do not require a cyber security strategy!
  - ❑ Rather a business strategy that incorporates cyber.
- ❑ Recognise Dave – some say he is 90% of the risk.
  - ❑ Ensure the main focus is not on the 10%.
- ❑ It’s the way you tell ém!
  - ❑ Communicate in business speak.
- ❑ Remember it’s enterprise wide
  - ❑ Position cybersecurity as a business and commercial issue rather than just an IT one.

Thank you!!

allan@internetworking4u.co.uk   @allanboardman   www.linkedin.com/in/allanboardman