

WannaCry

How to manage a cyber crisis

Richard Cumbley
Vanessa Havard-Williams
Tom Cassels
Peter Church

May 2017

How to manage a cyber crisis

Agenda

1. A ten minute primer on WannaCry
2. Crisis response and governance

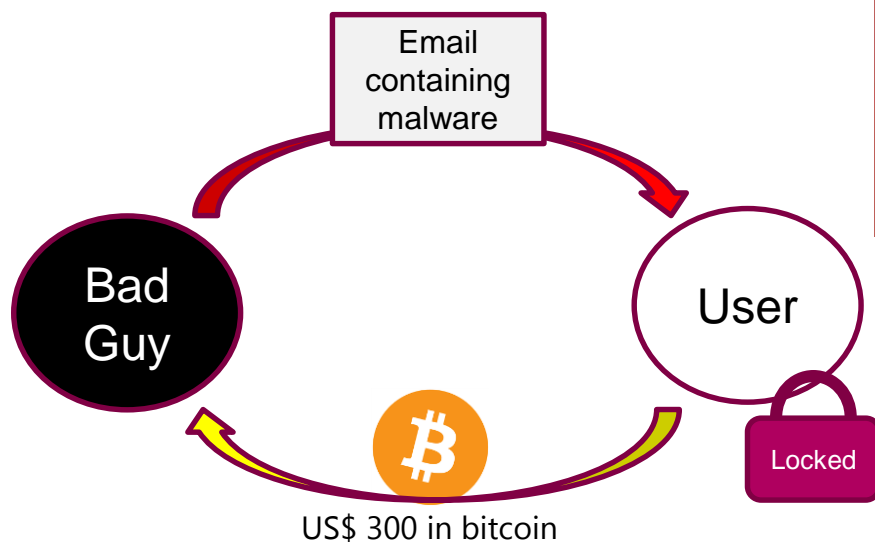
*"First you have to get the cow out of the ditch.
Second find out how the cow got into the ditch.
Third make sure you do whatever it takes so the
cow does not go in the ditch again"*

A ten minute primer on WannaCry

Starts with a standard ransomware attack...

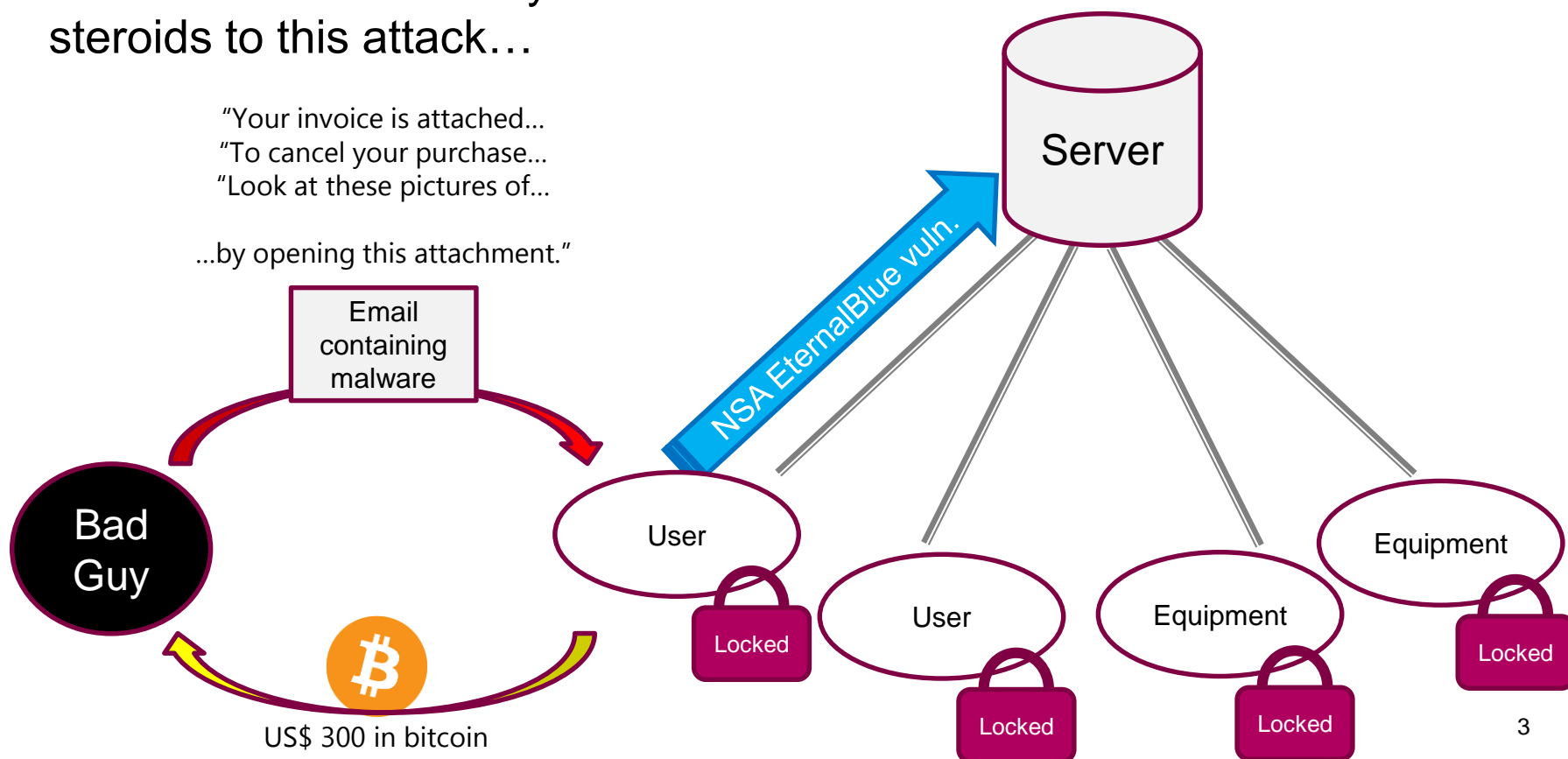
"Your invoice is attached...
"To cancel your purchase...
"Look at these pictures of..."

...by opening this attachment."



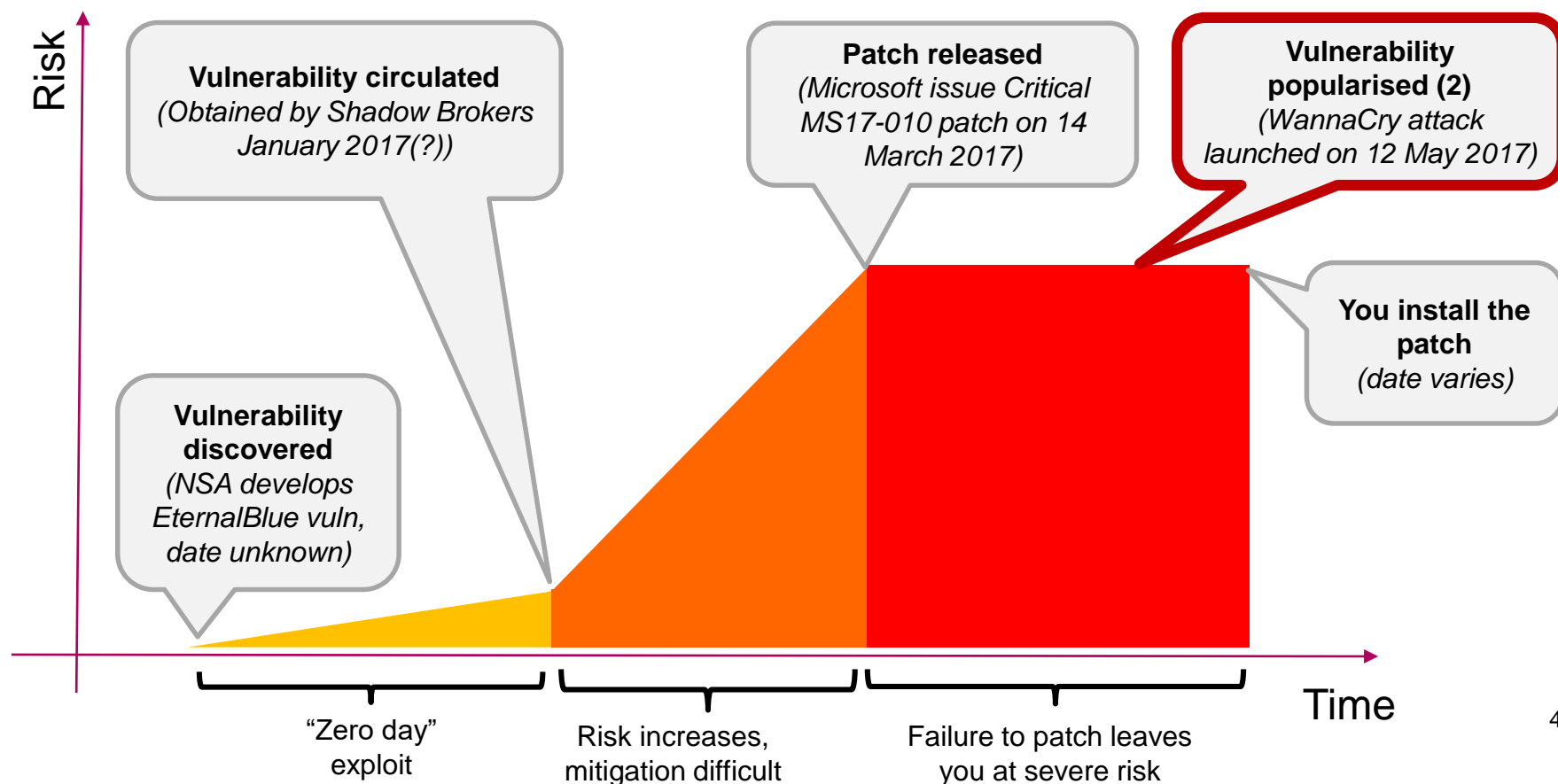
A ten minute primer on WannaCry

EternalBlue vulnerability adds steroids to this attack...



A ten minute primer on WannaCry

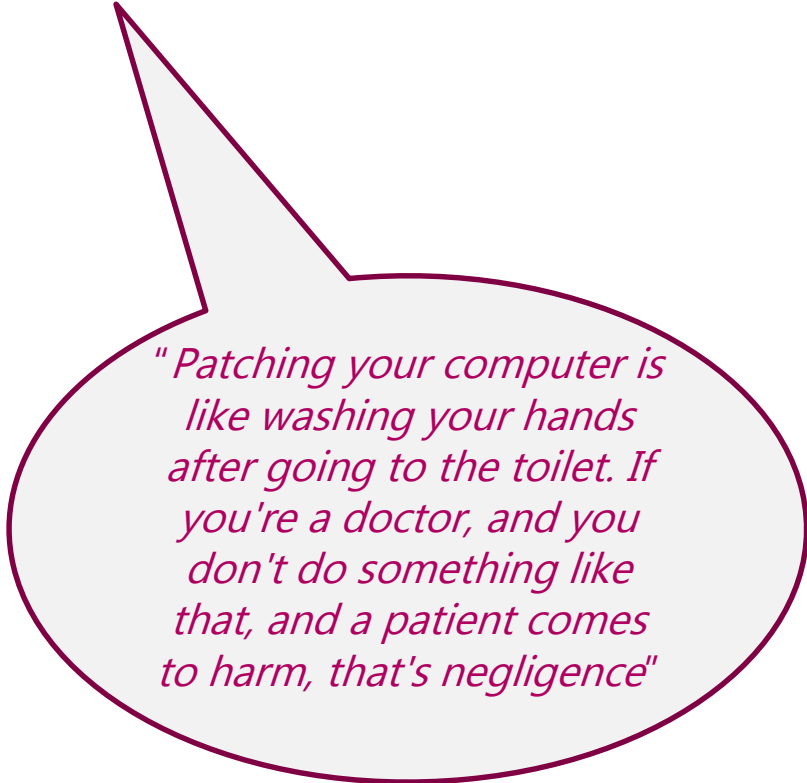
What is my risk profile?



A ten minute primer on WannaCry

So why does it take 58 days to apply a patch?

1. You need time to fit this into your patching cycle and to apply the patches
2. Patches aren't available



"Patching your computer is like washing your hands after going to the toilet. If you're a doctor, and you don't do something like that, and a patient comes to harm, that's negligence"

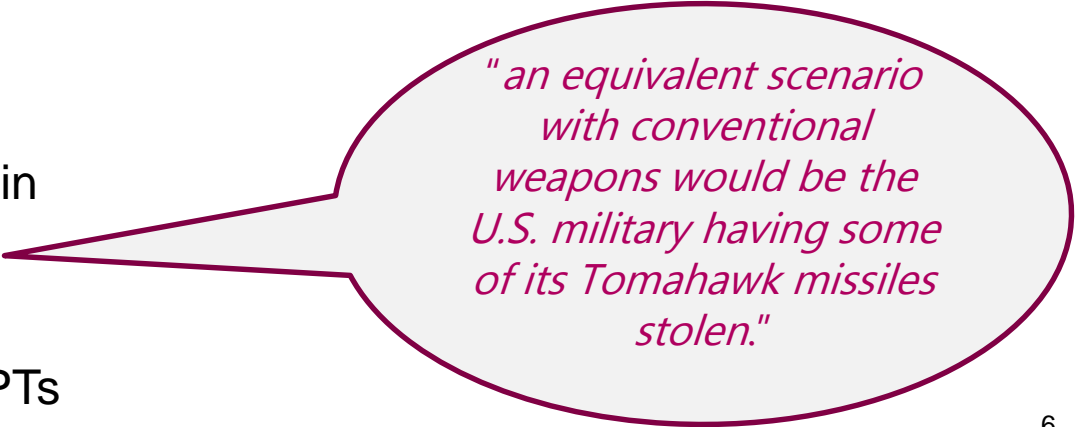
A ten minute primer on WannaCry

Technical and operational measures

1. Run supported software and apply patches in a timely manner
2. Run supported software and apply patches in a timely manner
3. Train (and test?) employees on IT security
4. Use of firewalls, email scanning, virus detection and control code execution
5. Ensure you back up data in a secure and separate manner

Bigger picture issues

1. Time to move to the cloud?
2. We need to talk about bitcoin
3. Government stockpiling of “zero-day” exploits
4. Cyber warfare and other APTs



"an equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen."

Crisis response



Governance: mitigating your risk exposure

Board oversight: informed understanding of the organization's cyber security position and strategy, resourcing, culture and residual risk profile

Adequate resourcing: CISO with appropriate reporting line/seat at management committee, and technical, human and financial resources. Up to date risk and asset assessment and cyber/privacy strategy.

Implementation & culture: adequacy of training, regulatory and policy compliance and enforcement. Retirement of unsupported or outlier software. Process to pick up issues, patches etc Supplier engagement :

Monitoring and Verification: Reporting and auditing of compliance requirements, issue management, engagement of supply chain. Review by Exco and Board.

Incident response and reporting: rehearse approach to cyber incidents including mapping regulatory and other notification obligations. Use findings to inform strategy: continuous improvement...

Linklaters LLP

One Silk Street

London EC2Y 8HQ

Tel: (+44) 20 7456 2000

Fax: (+44) 20 7456 2222

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The term partner in relation to Linklaters LLP is used to refer to a member of Linklaters LLP or an employee or consultant of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications. A list of the names of the members of Linklaters LLP together with a list of those non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, One Silk Street, London EC2Y 8HQ or on www.linklaters.com and such persons are either solicitors, registered foreign lawyers or European lawyers. This document contains confidential and proprietary information. It is provided on condition that its contents are kept confidential and are not disclosed to any third party without the prior written consent of Linklaters. Please refer to www.linklaters.com/regulation for important information on our regulatory position.