RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

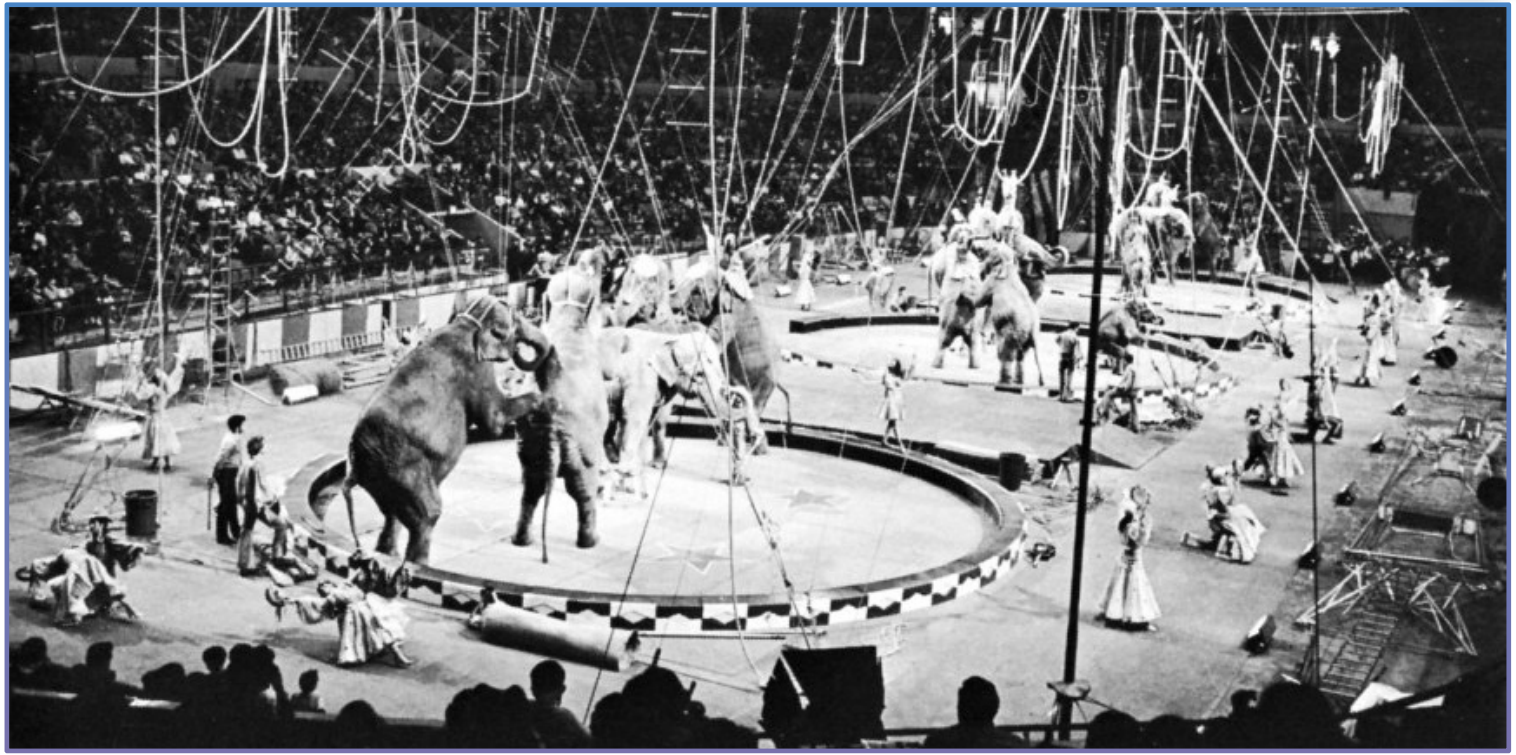
SESSION ID: CXO-W04

LEARNING FROM THE 3-RING CIRCUS OF NOT-PETYA

Todd Inskeep

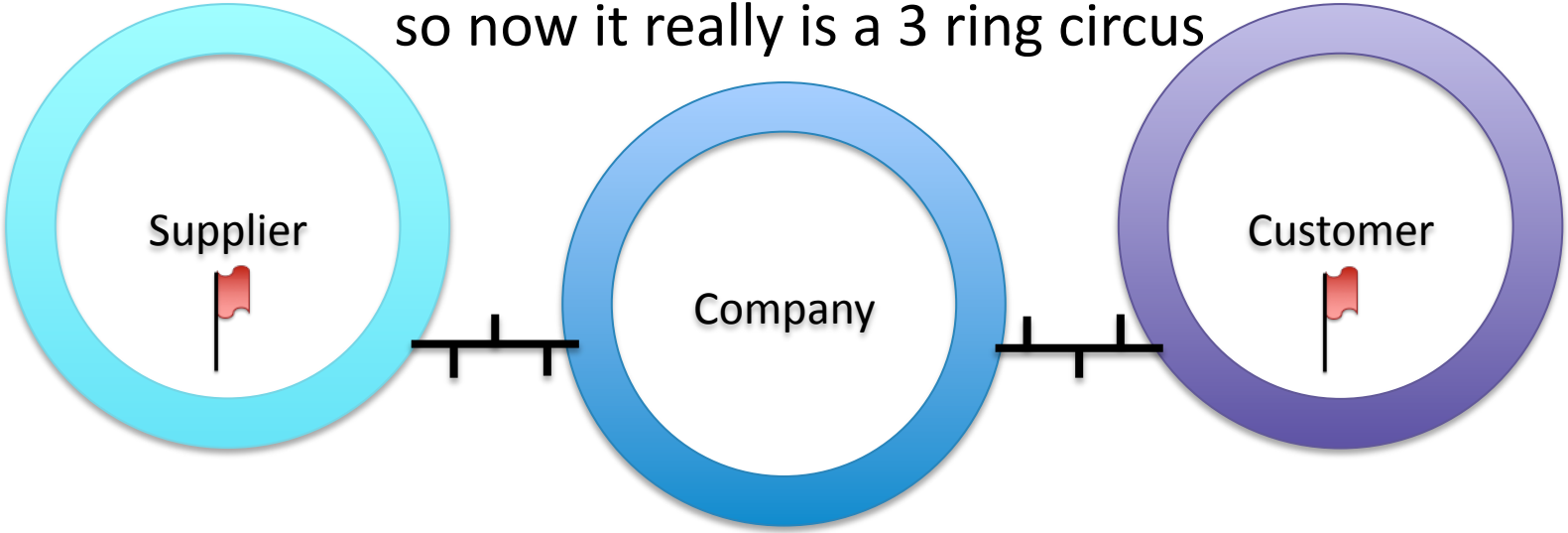
Principal
Booz Allen Hamilton
@Todd_Inskeep

June 27 seemed like an ordinary day



Then the email started

so now it really is a 3 ring circus



By the time we were reading email it was too late

But we didn't know that yet

Decision Point One

Do we sever connections?

What is our plan to reconnect?

Lessons Learned Part 1: Before an Event

- Verify your Business Continuity Plan
  - Know your real business dependencies
  - Cover the full range of BC planning
  - Review your recovery timelines and expectations
  - Consider an out-of-band network with critical applications and data
  - Practice for different events, use tabletop exercises
- Ensure you have offline access to incident response and BC plans
- Build relationships with CISOs, ISACs, & others

- Document your external partner network connections
  - Plan for disconnecting & being disconnected
- Implement or review multifactor authentication for administrators
  - Evaluate privileged access management practices
- Start network segmentation & hardening
  - Especially manufacturing & OT environments
- Doublecheck phishing protection

So now the clowns start coming out

It will be a full day before good information is available

Reference NH-ISAC Paper

- https://nhisac.org/nhisac-alerts/petya-ransomware-updates/ -
- https://nhisac.org/wp-content/uploads/2017/07/white-paper-sharing-info-in-times-of-industry-crisis.pdf

And now the business is starting to call

- Supplier cannot ship
- Customer does not need services
- Product is backing up
- Significant revenue losses
- Business Continuity Plan

Decision Point Two: How do you respond?

Solve with the business

- Rebuild business capability
- Establish key decision parameters
- Restore onsite teams
- Plan restoration of normal services

Address as IT / IS

- Determine Priority:
  - Resolution or Investigation
- Spin up Intelligence Activities
- Notify Executive Committee
- Plan Remediation

What if you were the victim?

Mobilize additional resources

Who ya gonna call?

Forensics → Root Cause Analysis

Incident Response → Coordinate Activities

Threat Intel & ISAC Activity → Learn & Share

Adversary Hunt → Check on Secondary Concerns

Investigation Reporting → Recommendations

Remediation

Lessons Learned Part 2: During an Event

- Establish a 24x7 cyber command center for recovery efforts
  - You have to move forward, despite ambiguity (or sheer chaos!)
  - Add resources! You do not have enough
  - Incident fatigue sets in quickly
- The first information about the incident is wrong!
- You will quickly learn critical business processes
- Develop a risk-based and value-based recovery strategy

- Intensify 24x7 SOC/IR/TI monitoring
  - So you're not attacked while you're in recovery
- Details matter – specifics are critical

So what really happened?

April | **May** | **June** | **June 27, 2017**

ME.Doc Corp Server

Compromised Software Update Distributed

Early Malware Downloaded & Run

Data Exfiltrated

Compromised Software Final Update

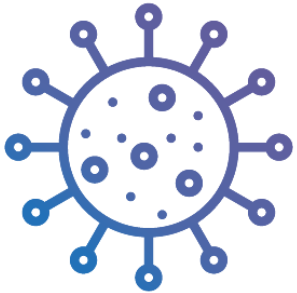
Command & Control

NotPetya Malware

various sources, including http://blog.talosintelligence.com/2017/07/the-medoc-connection.html

Not Petya Details

NotPetya Malware



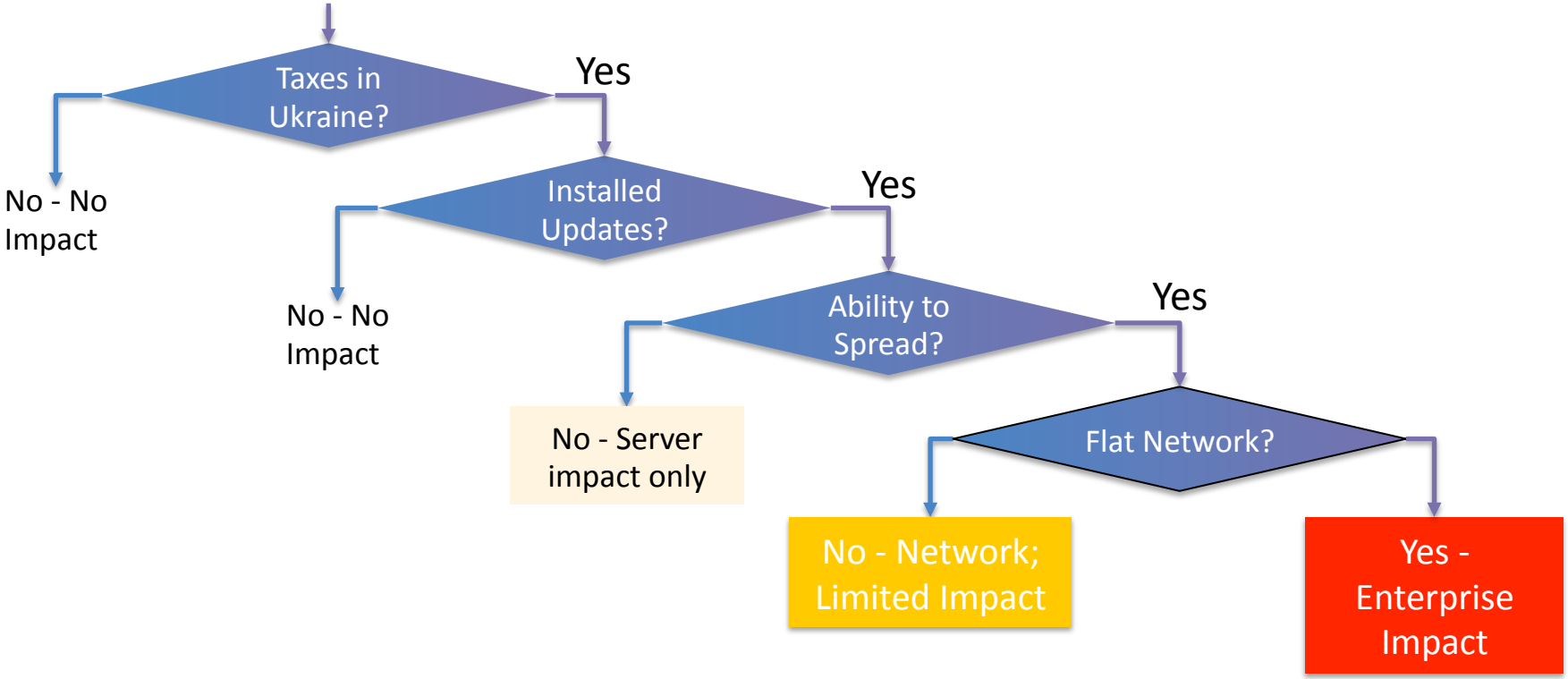
- Checks for existing copy, privileges, and AV Tools
- Anti-Forensics
- Schedules reboot 30/60 min
- Steals credentials; impersonates privileged user
- Distributes malicious file
- Executes file remotely To grow exponentially

→ Reboot corrupts Master Boot Record & Master File Table --> blank computer

> 10,000 PCs/min

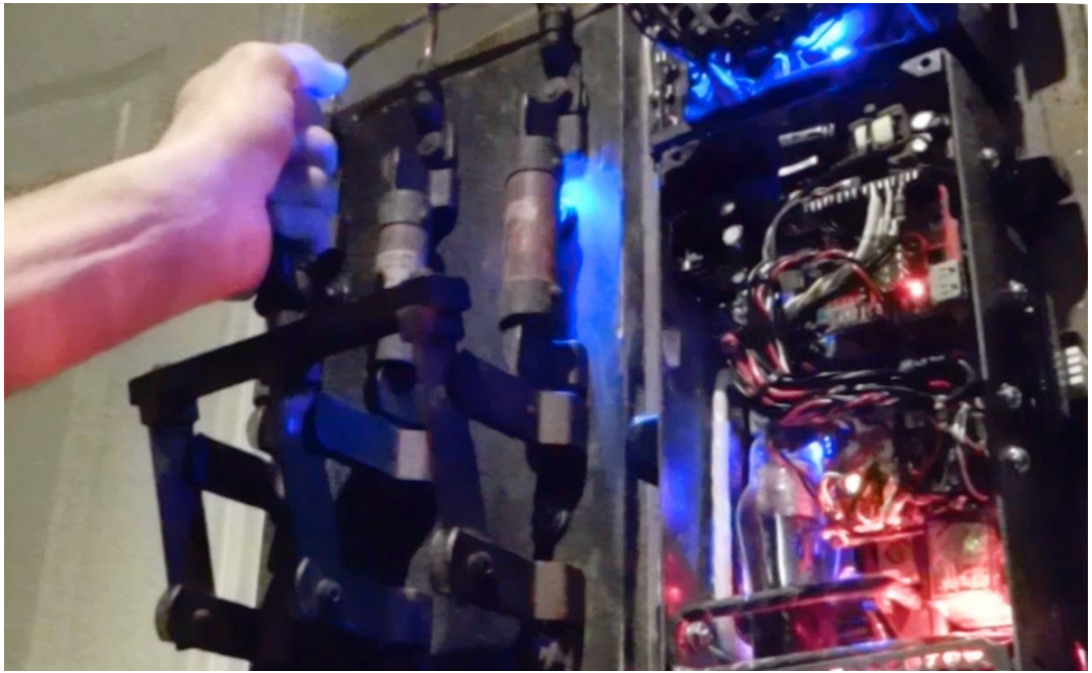
various sources, including
https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/

What drove the impact?



Decision Point Three: Restoring Normal Operations

Process to restore operations



Lessons Learned Part 3: After the Event

- You need a ***Business*** Continuity Plan; not an IT backup plan
- You need offline backups; NotPetya hit both sides of Hot-Hot solutions
- Revisit the 'Windows Monoculture'
- Assess your third-party software update process
- Manufacturing and Operational Technology systems are often running on unpatched legacy systems

- Fix foundational hygiene
  - ***Admin & PAM hygiene***
  - Harden Endpoints and use Next-Gen A/V
  - Continuous Vulnerability Management
  - Drive security upgrades across IT and OT environments
- Plan advanced security projects
  - User and entity behavior analytics
  - Logging & visibility
  - ***Real Segmentation***

Final Lesson:
Review Your Control Effectiveness

Typical Attack Chain	Attack Actions	Controls & Effectiveness
External & Internal Research	▪ What are attackers and attacks doing NOW? ▪ What trends are changing attacker actions and behavior? ▪ What's new or different at each stage?	▪ What controls are effective NOW? ▪ What controls can adjust to changing attacks? ▪ What's specific to preventing and detecting adversary activity at each stage?
Weaponization		
Delivery		
Exploitation		
Installation		
Command & Control (C2)		
Persistence/ Fullfilment		

Afterthought: Collateral Cyber Damage

- Historically, malware has impacted IT systems within a company
- WannaCry, Not-Petya illustrated something new: collateral damage

➢ Enterprise Risk Management needs to think about **Cyber** risks to the business *outside* the internal IT construct

Traditional Risk Management, plus Cyber

Business Risks

- Strategic Risks
- Financial Risks
- Marketing & Sales
- Operational Risks
- Reputational Risks
- Human Resource Risks
- Compliance, Regulatory & Legal Risks
- Catastrophic Risk
- Information Technology Risks
- ➢ ***Product Security***
- ➢ ***Cyber Risks***

Product Security Risks:

- Connected systems & devices
- Business models now require security
- Don't forget services & *privacy*

Cyber Security Risks:

- Business now depends on doing security well, internally & externally
- Business dependencies on partner IT systems and operations may not be obvious

When you get back to the office

- Review how Enterprise Risk Management addresses cyber risk
  - Is there a new need for corporate education on collateral damage
- Review blocking and tackling in IT & IS
  - Versioning, Vulnerabilities & Patching, PAM, network segregation
- Triangulate on Business Dependencies on outsourced technology
  - What critical suppliers have significant technology dependencies
- Build real *Business* Continuity Plans
  - Update Backup & DR Plans
  - Test the plans against multiple scenarios over time
- Practice and prepare for worst case scenarios