A Security Mindset
in the Age of Ransomware

Royce Williams

ACP Alaska Chapter – April 4, 2018

Overview

About me

The existential threat
The will
The attack graph
Resilience

Questions

About me

$DAYJOB in InfoSec in the telecom sector

ISP scars

Independent security researcher

Password auditor and enthusiast

The existential threat

Old risks - made visible by new levels of impact

The will to change

Ransomware has stimulated renewed interest in accelerating change

Policies and procedures support that change – culturally and operationally

P&P clarify the structure of change, removing ambiguity

The will to change

Other methods to endorse and encourage change:

- Leading by example (from the top)
- Constructiveness
- Flexibility
- Increasing awareness

The attack graph

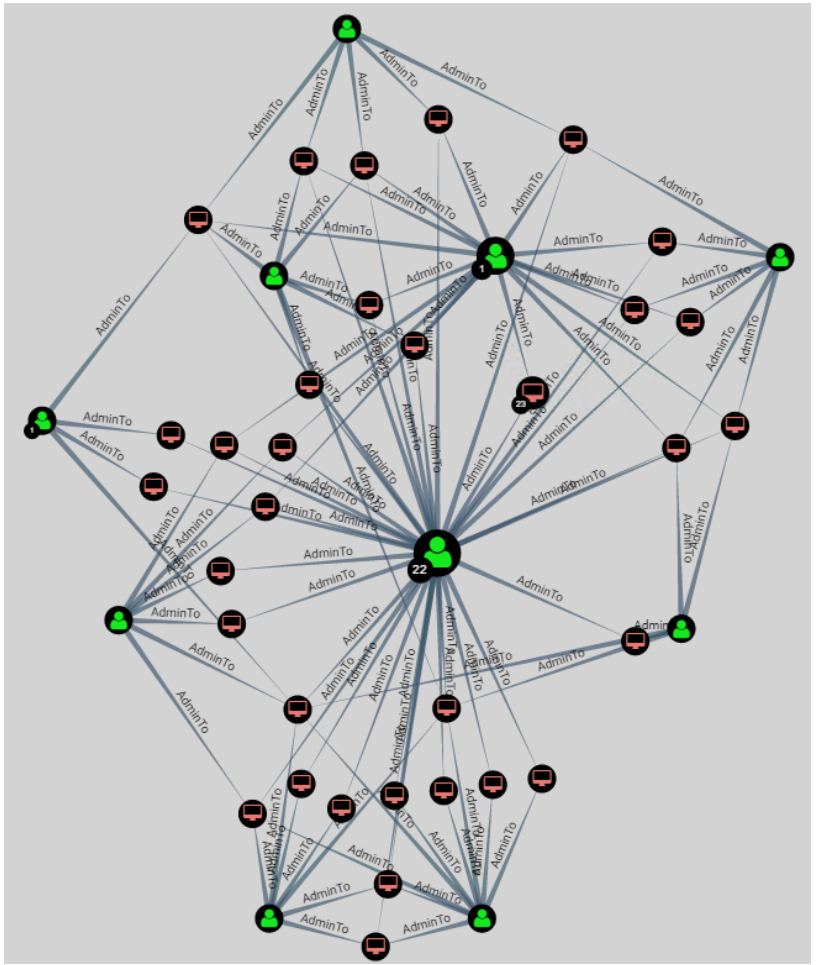
Defenders think in *lists*.
Attackers think in *graphs*.

As long as this is true, attackers win.

- John Lambert, Microsoft Threat Intelligence Center

https://blogs.technet.microsoft.com/johnla/2015/04/26/defenders-think-in-lists-attackers-think-in-graphs-as-long-as-this-is-true-attackers-win/

The attack graph – attacker mindset



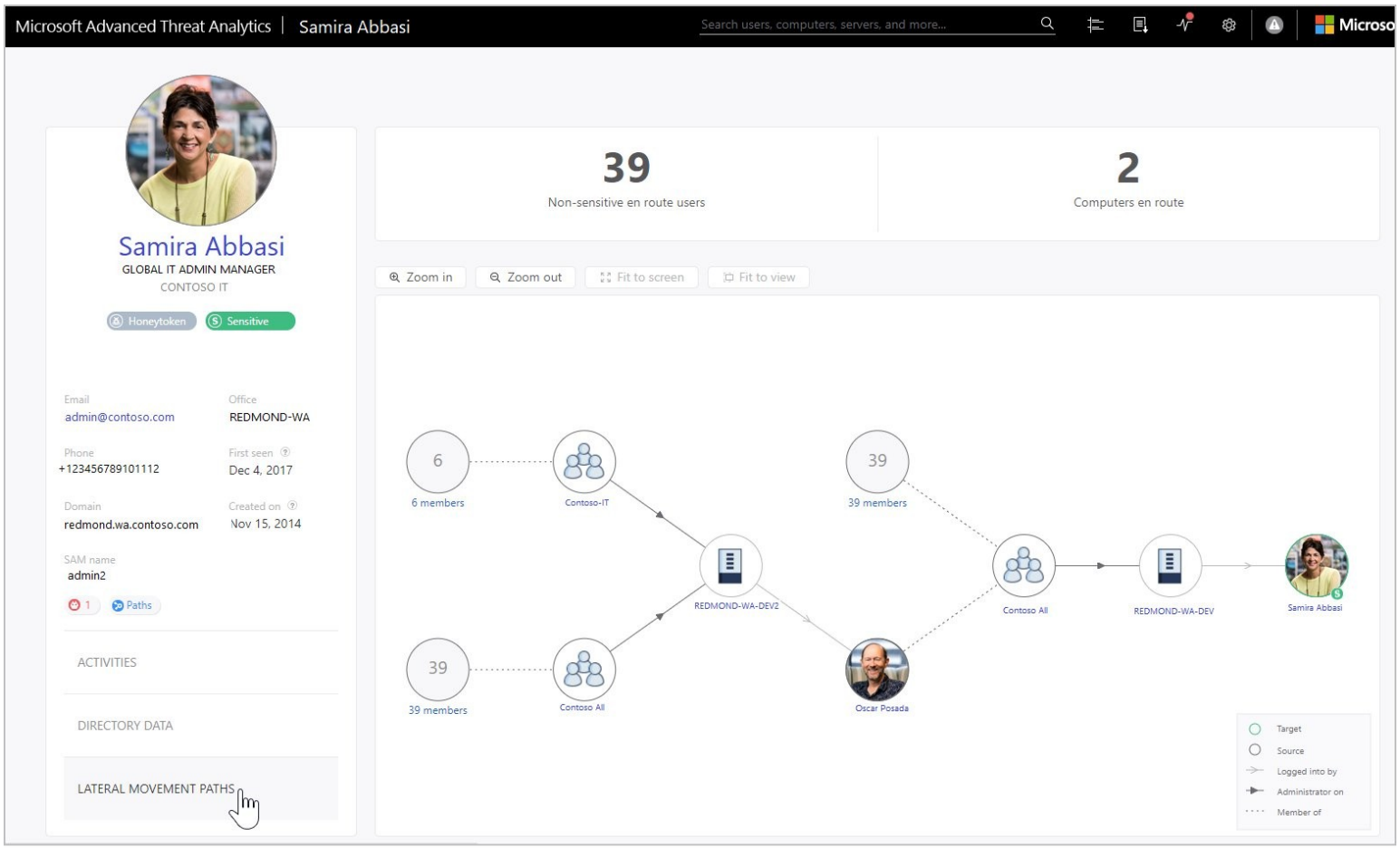
Good: Find *any* path boxes that will get you to your target

Better: Find *all* such paths

https://github.com/BloodHoundAD/BloodHound

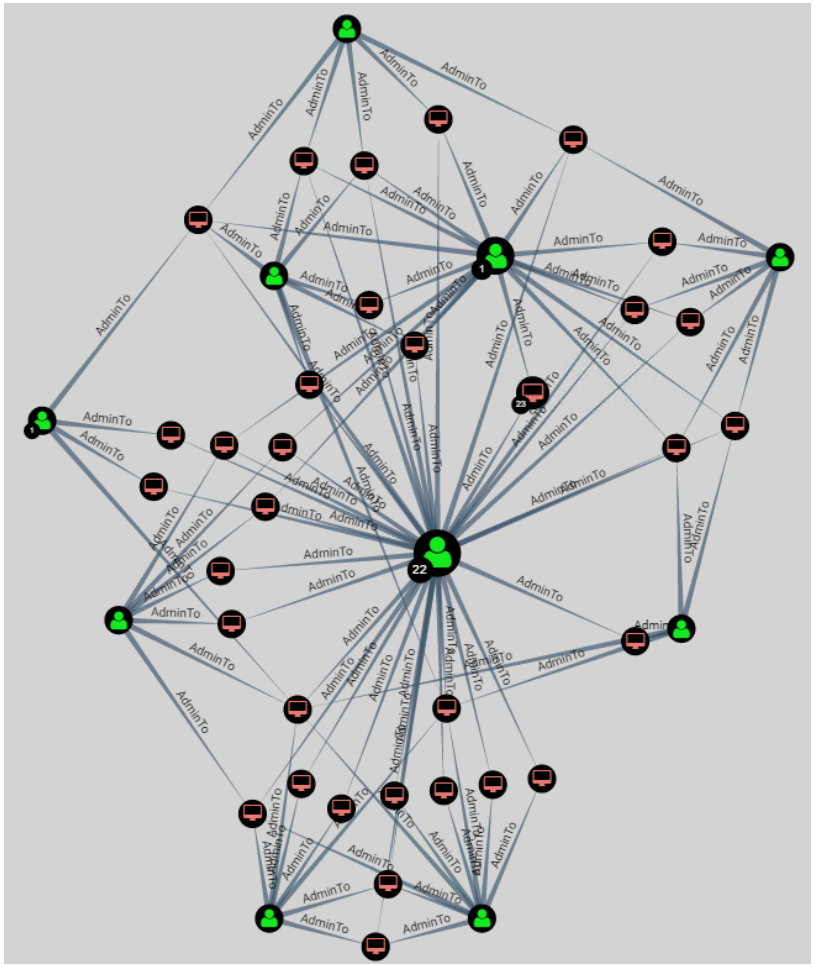
Image source: https://blog.stealthbits.com/local-admin-mapping-bloodhound

The attack graph – defender mindset



Source: https://twitter.com/TalBeerySec/status/977873572671688706

The attack graph – defender mindset



Good: Track down all vulnerable systems and fix them … for this one vulnerability

Better: Eliminate *entire classes of attack*

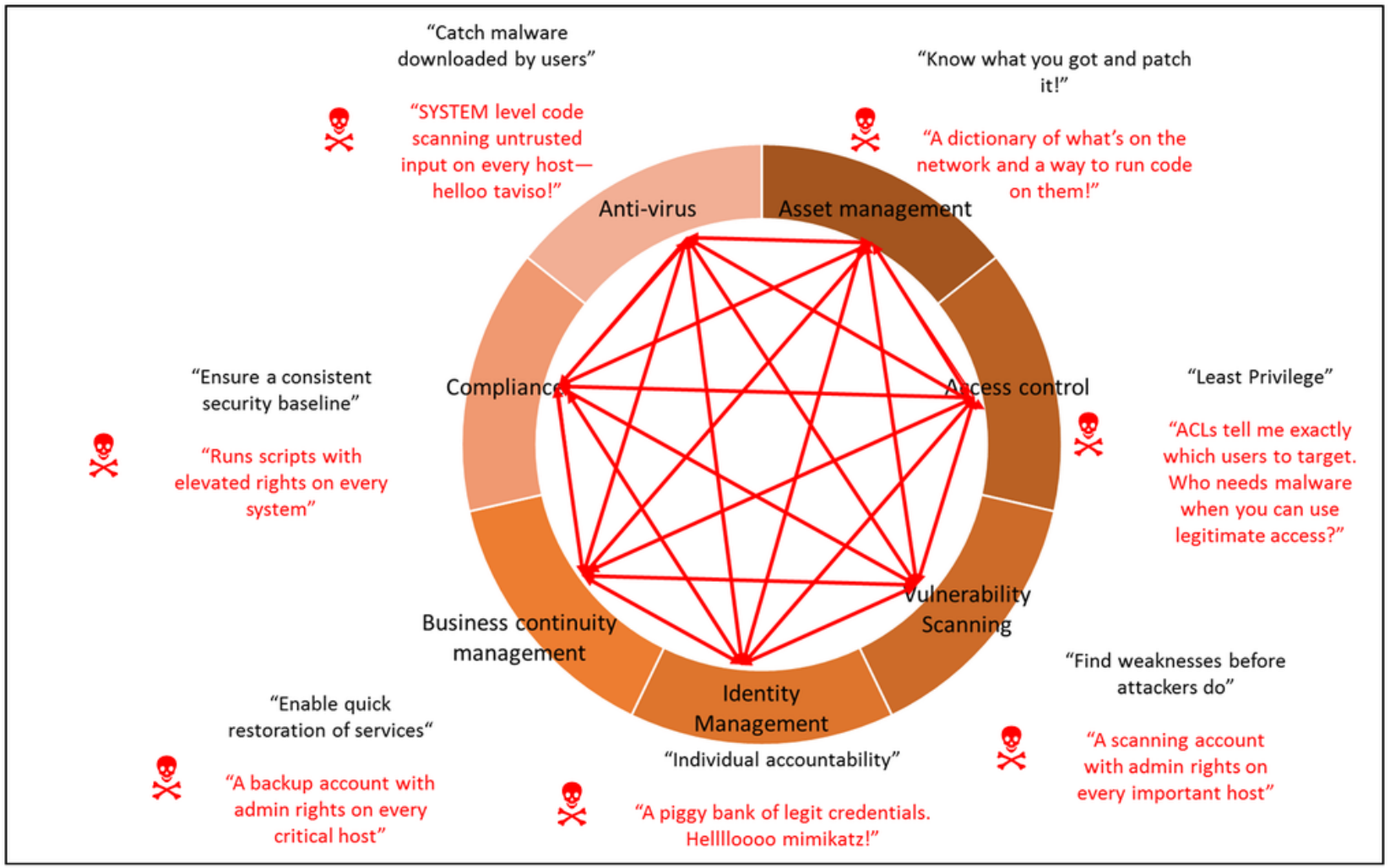
Source: https://blog.stealthbits.com/local-admin-mapping-bloodhound

Beware the Attack Surface of InfoSec by @JohnLaTwC

Traditional defenders see security controls as solving InfoSec problems.

Attackers see security controls as an attack graph of points of compromise.

See Both.



The attack graph – attacker mindset

Hiding backups from the bad guys

Cyber extortionists know that backups are their number one enemy and are adapting their ransomware to look for them.

"Several ransomware families destroy all Shadow Copy and restore point data on Windows systems," said Noah Dunker, director of security labs at RiskAnalytics "Many ransomware families target all attached drives, and happen to encrypt the backups as well, though not likely by design."

Any file system that's attached to an infected machine is potentially vulnerable, as well as attached external hard drives and plugged-in USB sticks.

Problem: Companies can refuse to pay ransoms if they can restore from backups

Solution: *Destroy the backups*

Source: https://www.csoonline.com/article/3075385/backup-recovery/will-your-backups-protect-you-against-ransomware.html

The attack graph – attacker mindset

Attackers:

- Know more about your network than you do
- Are constantly expanding and improving methods (that you cannot predict)
- Have strong incentives to achieve their goals
- Will take *any path to that goal*

Resilience

The capacity to recover quickly from difficulty; toughness.
(Oxford)

An ability to recover from or adjust easily to misfortune or change
(Merriam-Webster)

The power or ability to ***return to the original form****, position, etc., after being bent, compressed, or stretched; elasticity.*
(Dictionary.com)

Fostering resilience

Enable policies and culture that support:

- Reducing complexity … *without eliminating biodiversity* (analog/alternate methods – Dan Geer, 'A Rubicon')

> have now, at least so long as we demand freedom. Countries that built complete analog physical plants have a signal advantage over countries that leapfrogged directly to full digitalization. The former countries have preservable and protective firebreaks in place that the latter will never have, but the former countries enjoy their resilience dividend if, and only if, they preserve their physical plant. That such preservation can deliver both resilience for the digitalized and continued freedom for those choosing not to participate in digitalization is unique to this historical moment.

Fostering resilience

Enable policies and culture that support:

- Reducing *accidental* complexity (Brooks)

*Accidental complexity relates to problems which **engineers create** and can fix; for example, the details of writing and optimizing assembly code.*

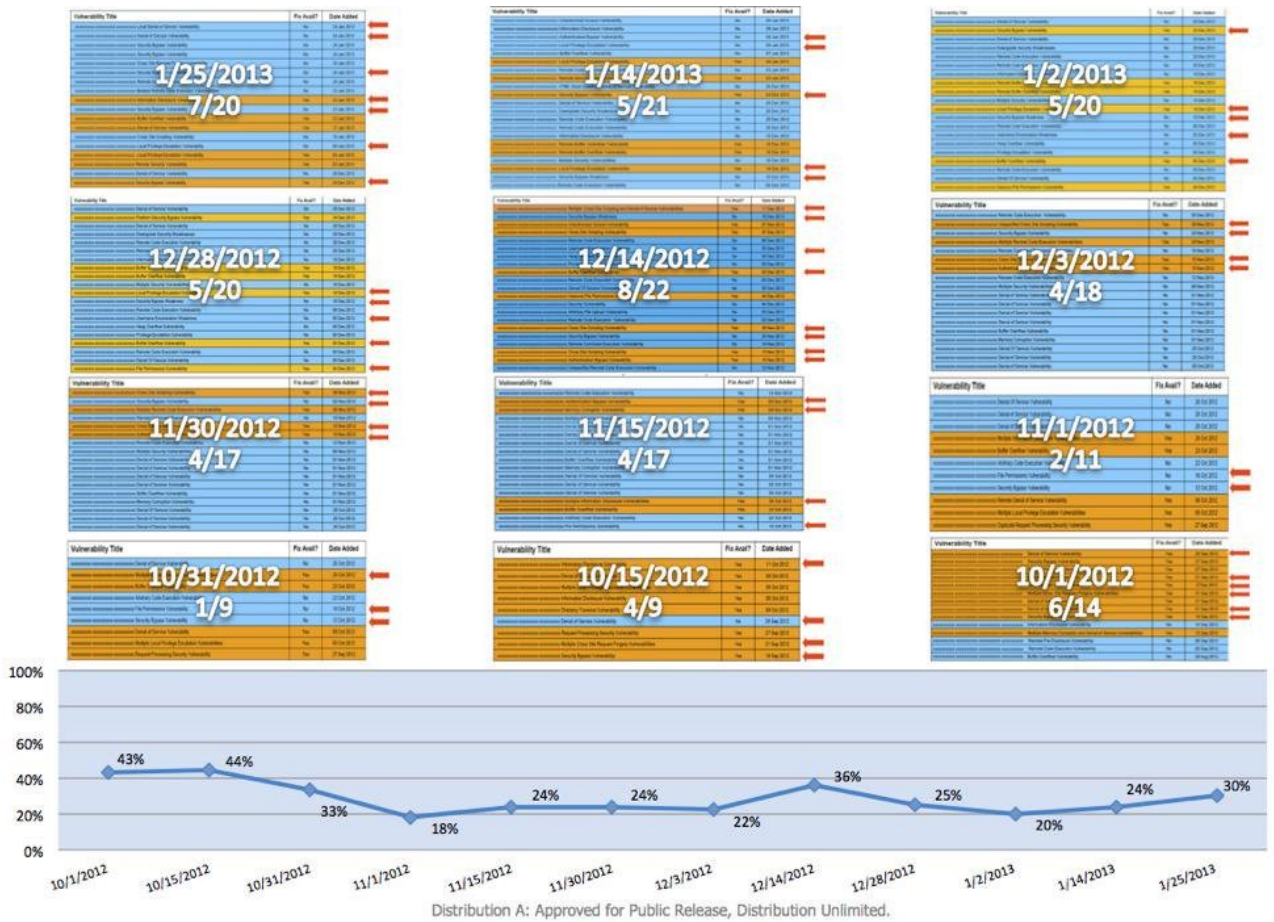
Essential complexity is caused by the problem to be solved, and nothing can remove it.

(source: Wikipedia, 'No Silver Bullet')

Controls … *as attack surface*

"DoD data (cleared for release) shows on average **1/3** of vulns in government systems is in the security software."
- @dotMudge

(Security solutions often have significant *accidental complexity)*

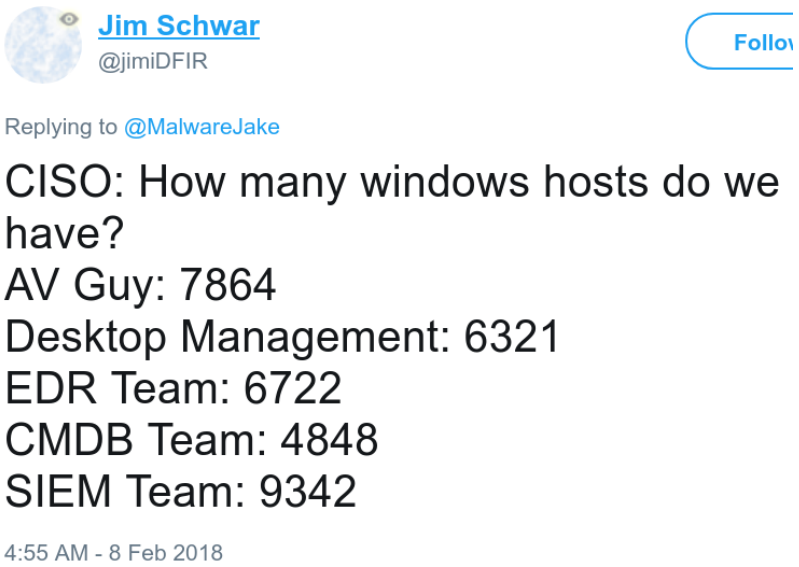


Fostering resilience

Enable policies and culture that support:

- Increased visibility (SIEM, sysmon / config, Powershell logging)
- Seeing what the attacker sees – rolling inventory, battle map, attack graph
- Discovery and elimination of entire classes of attack (map .js to Notepad)

Fostering resilience



Security teams can see what no one else can (except for the attacker!)

Measuring Resilience
(cyber domain)

	Prepare	Absorb	Recover	Adapt
Physical	Percent of malware attacks blocked by firewall	Percent of system affected before threat is contained	Time between event and return to computer's optimal performance	Amount of memory reserved for future system changes
Information	Percent of system components monitored for attack	Time for computer to locate software needing repair and to prepare resources	Time for software to distribute resources in order to recover properly	Ability of system to anticipate future system states
Cognitive	Plans for storage and containment of classified or sensitive information	Ability to evaluate system performance during attack and determine if mission can continue	Decision-making protocols to select recovery options	Existence of methods for determining motive for attack
Social	Degree of training for cyber-security awareness among system users	Lines of communication between identified experts and resilience personnel	Level of liability or loss of confidence in the organization	Methods for information sharing among system users and system managers about emerging threats and protection measures

Table 3. Cyber resilience matrix, cyber attack

Source: "Resilience Metrics: Lessons from Military Doctrines", thesolutionsjournal.com

The only cyber security principles that are known to work (thegrugq)

- Increase the cost of the compromise
- Decrease the value of the compromise
- Restrict adversarial freedom of movement post compromise
- Increase ease of detecting a compromise
- Increase chance of detecting a compromise
- Audit trails for post compromise analysis
- Vigilance

Source: https://medium.com/@thegrugq/security-cyber-and-elections-part-3-9398f639aa28

Thanks

Kevin Beaumont | Dan Geer | John Jenkinson |
John Lambert | mudge | Jan Schaumann | thegrugq

Internet Alaska | ACS | Alaska USA | Alyeska Pipeline | GCI

Contact: **royce@techsolvency.com | @TychoTithonus**

Slides, errata, references:
`www.techsolvency.com/talks`