THE UNIVERSITY OF AUCKLAND
Te Whare Wānanga o Tāmaki Makaurau
NEW ZEALAND

The Hidden Fortress

Defending large networks and complex organisations with agile security

Hinne Hettema
IT Security team leader, University of Auckland
h.hettema@auckland.ac.nz

April 2016

root@FirstTC2016:~# whoami

Theoretical chemist and philosopher by training
Wrote DALTON program code [in FORTRAN]
Played with supercomputers such as Cray Y-MP
First got hacked in 1991
Worked 15 years as IT Infrastructure architect for various NZ companies
Now lead the IT Security team @UoA by day
Lecture in cyber security at Unitec

The agenda

A view from an operational security team…

Three Contexts
Agile Security
Building the team
Team practices
Examples

Some numbers

NZ$ 1 Billion turnover
700,000 identities
40,000 current students
5,000 staff
3,700 servers
350 web applications
1 big target

…n Bergen auf Zoom Anno Dñi 1583 am 9 vnd 10 Mey
Drumb mit Fitzrecht er procidirt
Den Capitein examinirt
Leist im brengen vnd gutt vnd leben
Das er dass haus so baldt ergeben
WOVDE

We are already hacked

Almost every day the security team finds things on our network that shouldn't be there

THE UNIVERSITY OF AUCKLAND
Te Whare Wānanga o Tāmaki Makaurau
NEW ZEALAND

Three Contexts

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

— Sun Tzu, The Art of War

Cybersecurity problem

Very poorly understood
Many definitions, none of which do the job
Can easily become an industry of overinflated claims

My definition: cyber insecurity occurs when there are ‘bumps’ in the interactions between three relevant contexts:

1. Business context (People, Process,…)
2. Technology context
3. Attack | Defence context

Failure modes

The cyber ‘bump’ or ‘failure mode’ usually is

- Gaps and vulnerabilities in technological defences
- Inconsistencies, for instance between process and technology
- Wrong incentives, leading to the wrong decisions
- An attractive environment for cyber criminals

Example: Phishing

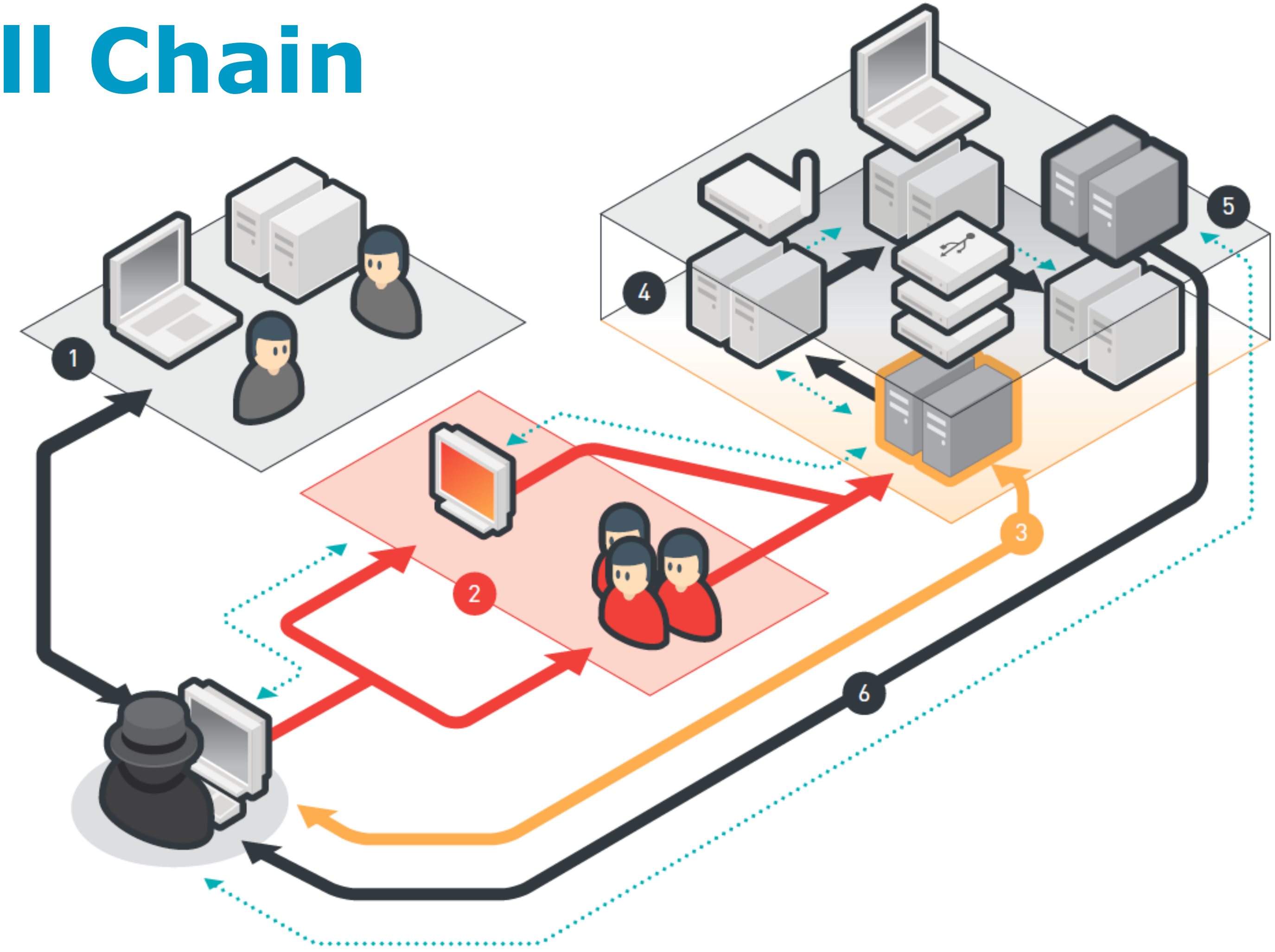
An attacker sends an email to a user
Which looks like a ‘regular’ email to that user
Supporting some business process
Technology checks (DKIM, SPF) on verifying email are difficult, inconsistently applied, and quite often ignored
Browsers on mobile devices often do not use the ‘smartscreens’ which warn users of phishing pages
And detection practices are not up to the task

What drives attacks?

Unlike ‘acts of god’ attacks are **intentional**

Very large economies of scale
Very low chance of getting caught
Very easy to do in different jurisdictions, so low chance of conviction
Methods and tools readily available

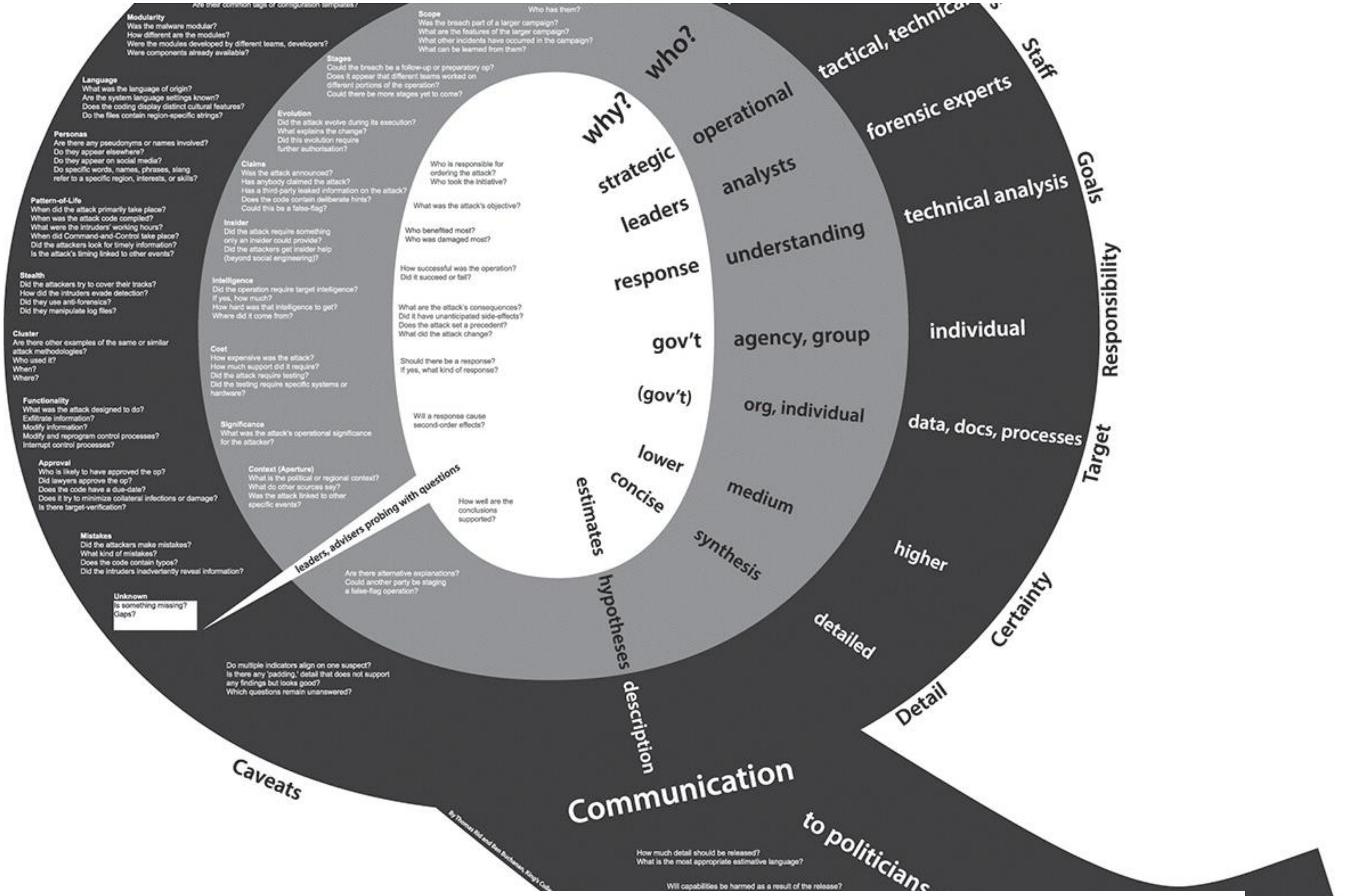
Kill Chain



1 Intelligence gathering
2 Point of entry
3 C&C communication
4 Lateral movement
5 Asset discovery
6 Data exfiltration
7 Maintenance

© http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/targeted-attack-campaigns-and-trends-2014-annual-report

Attribution



Are their common tags or configuration templates?

Modularity
Was the malware modular?
How different are the modules?
Were the modules developed by different teams, developers?
Were components already available?

Language
What was the language of origin?
Are the system language settings known?
Does the coding display distinct cultural features?
Do the files contain region-specific strings?

Personas
Are there any pseudonyms or names involved?
Do they appear elsewhere?
Do they appear on social media?
Do specific words, names, phrases, slang refer to a specific region, interests, or skills?

Pattern-of-Life
When did the attack primarily take place?
When was the attack code compiled?
What were the intruders' working hours?
When did Command-and-Control take place?
Did the attackers look for timely information?
Is the attack's timing linked to other events?

Stealth
Did the attackers try to cover their tracks?
How did the intruders evade detection?
Did they use anti-forensics?
Did they manipulate log files?

Cluster
Are there other examples of the same or similar attack methodologies?
Who used it?
When?
Where?

Functionality
What was the attack designed to do?
Exfiltrate information?
Modify information?
Modify and reprogram control processes?
Interrupt control processes?

Approval
Who is likely to have approved the op?
Did lawyers approve the op?
Does the code have a due-date?
Does it try to minimize collateral infections or damage?
Is there target-verification?

Mistakes
Did the attackers make mistakes?
What kind of mistakes?
Does the code contain typos?
Did the intruders inadvertently reveal information?

Unknown
Is something missing?
Gaps?

Do multiple indicators align on one suspect?
Is there any 'padding,' detail that does not support any findings but looks good?
Which questions remain unanswered?

Who has them?

Scope
Was the breach part of a larger campaign?
What are the features of the larger campaign?
What other incidents have occurred in the campaign?
What can be learned from them?

Stages
Could the breach be a follow-up or preparatory op?
Does it appear that different teams worked on different portions of the operation?
Could there be more stages yet to come?

Evolution
Did the attack evolve during its execution?
What explains the change?
Did this evolution require further authorisation?

Claims
Was the attack announced?
Has anybody claimed the attack?
Has a third-party leaked information on the attack?
Does the code contain deliberate hints?
Could this be a false-flag?

Insider
Did the attack require something only an insider could provide?
Did the attackers get insider help (beyond social engineering)?

Intelligence
Did the operation require target intelligence?
If yes, how much?
How hard was that intelligence to get?
Where did it come from?

Cost
How expensive was the attack?
How much support did it require?
Did the attack require testing?
Did the testing require specific systems or hardware?

Significance
What was the attack's operational significance for the attacker?

Context (Aperture)
What is the political or regional context?
What do other sources say?
Was the attack linked to other specific events?

Are there alternative explanations?
Could another party be staging a false-flag operation?

Who is responsible for ordering the attack?
Who took the initiative?

What was the attack's objective?

Who benefited most?
Who was damaged most?

How successful was the operation?
Did it succeed or fail?

What are the attack's consequences?
Did it have unanticipated side-effects?
Does the attack set a precedent?
What did the attack change?

Should there be a response?
If yes, what kind of response?

Will a response cause second-order effects?

How well are the conclusions supported?

How much detail should be released?
What is the most appropriate estimative language?

Will capabilities be harmed as a result of the release?

plication
the intruders respond
blicity?

© Thomas Rid & Ben Buchanan (2015) Attributing Cyber Attacks, Journal of Strategic Studies, 38:1-2, 4-37, DOI: 10.1080/01402390.2014.977382

Business response: fear

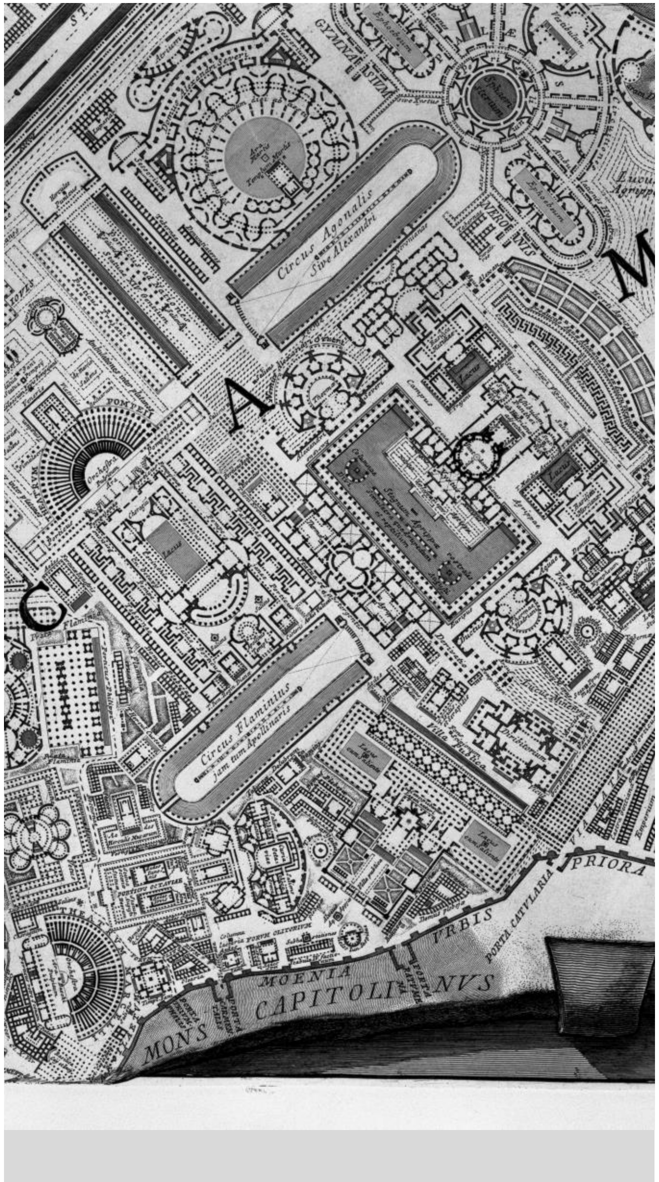
Operational Security dimension	Fear Based Model	Resilient model
Security posture	Reactive	Proactive
Incident approach	Panic [denial, anger, bargaining]	Controlled chaos
Security team HR	“we need a fall guy”	“we need a strong team”
Security monitoring	Haphazard [Worse] Vendor driven	Controls based on • attacker behaviour/movement • exploit risks • vulnerability/exposure
Predictability	None / little	Anticipated events
People impact	Burn-out	Busy
Security perception	IT problem Hackers are nerds doing bad things!	Business problem Hackers are people too
Defence focus	Border Fortress	Defence in depth Immune system Resilience

Agile Security

[…] As for the more direct question of what should be done, our figures suggest that we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response – that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail.

Ross Anderson, *Measuring the Cost of Cybercrime*, 2012

Aims and Goals



Secure by design
Secure in deployment
Secure in operation
Secure in breach

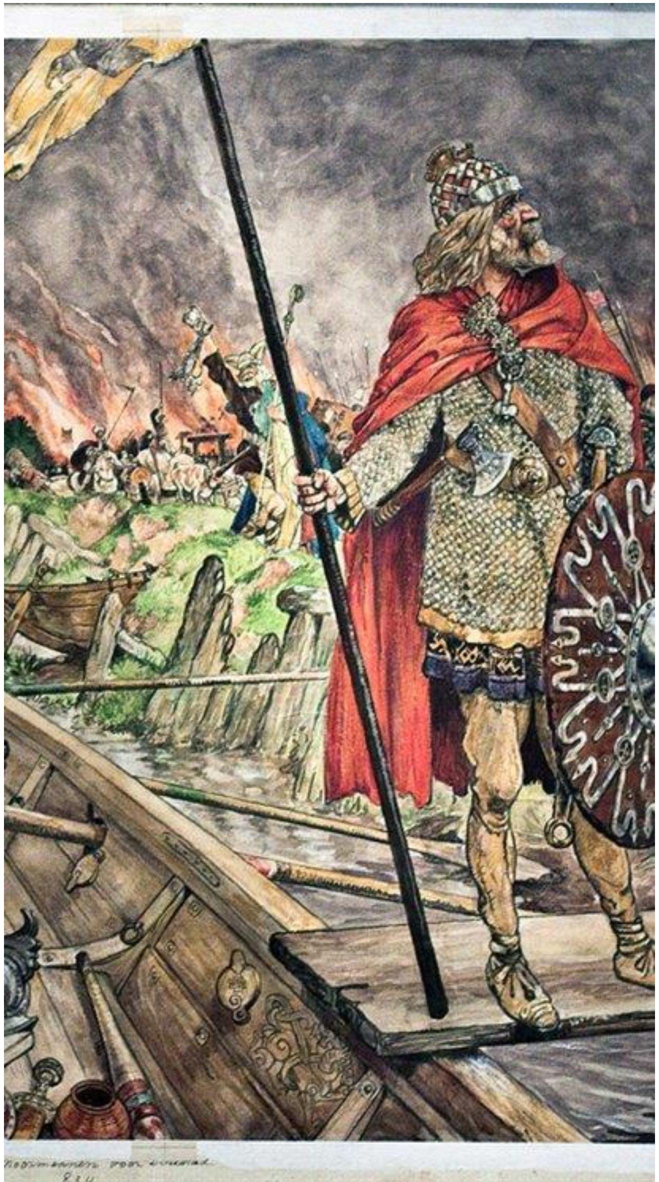
In Breach?

Many people only discover they’ve been hacked

- AFTER the attacker has achieved their objectives
- AFTER the attacker has started wrecking the place

hence

- AFTER the damage is done

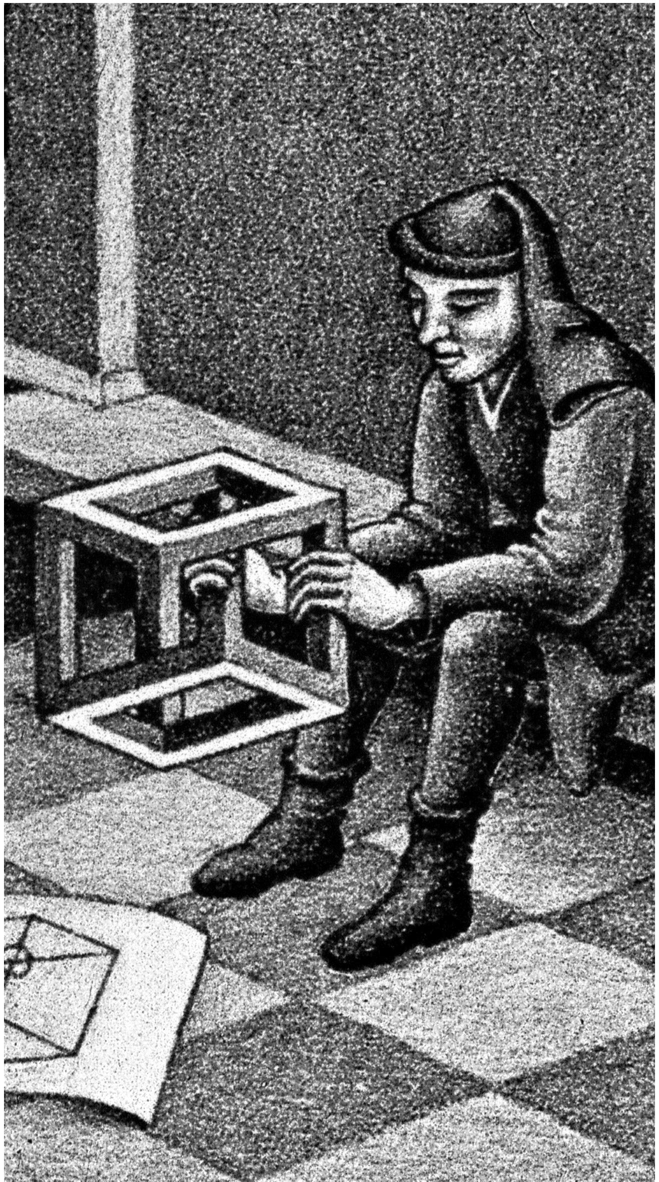


Solve me!

Four ‘build the case’ strategies

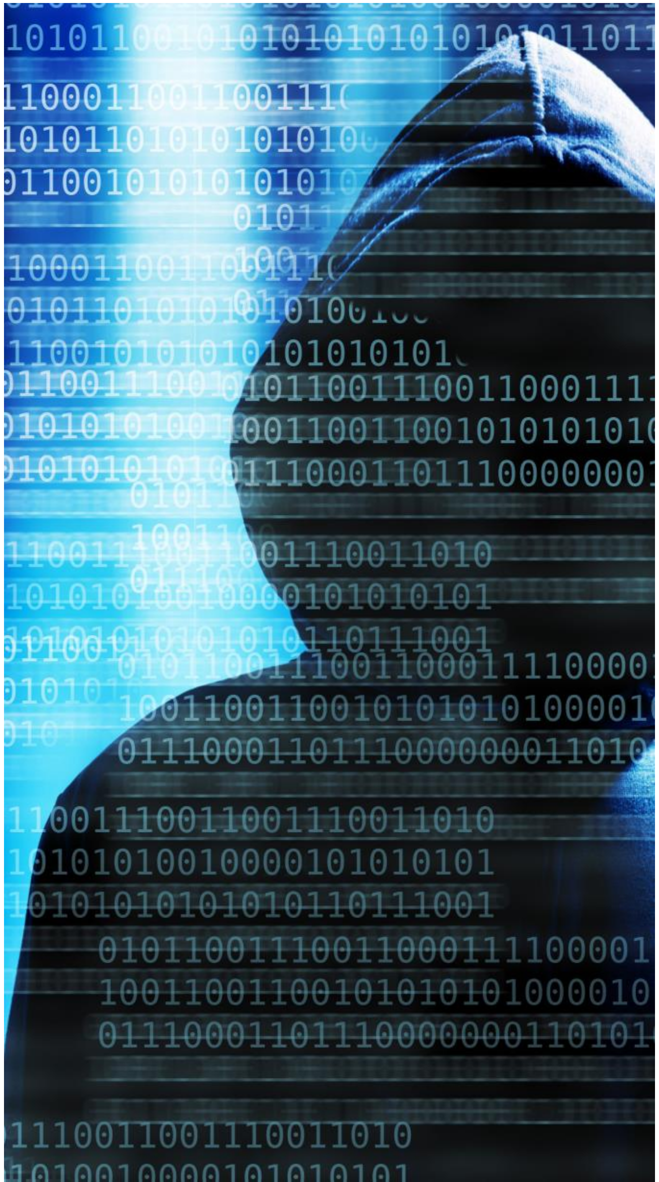
1. FUD bomb
2. Risk-based
3. Compliance-based
4. Guerrilla

1-3 are failures, 4 can be made to work



FUD Bomb: scare ‘n sell

Fear: “Hackers are everywhere and smarter than you. They are after you all the time. Are you afraid now? Good, you should be.”
Uncertainty: “Security is highly technical, and this thingy has a lot of blinking coloured lights”
Doubt: “No one got fired for buying …” / anything with “market leader”



Risk-based

1. Risk discussions force you into ROI discussions, which security always loses
2. Reason: security events are perceived as ‘black swans’, and no one invests in preparing for black swan events
3. ‘Three monkey strategy’ still effective for many organisations: don’t look and security events aren’t there

Compliance

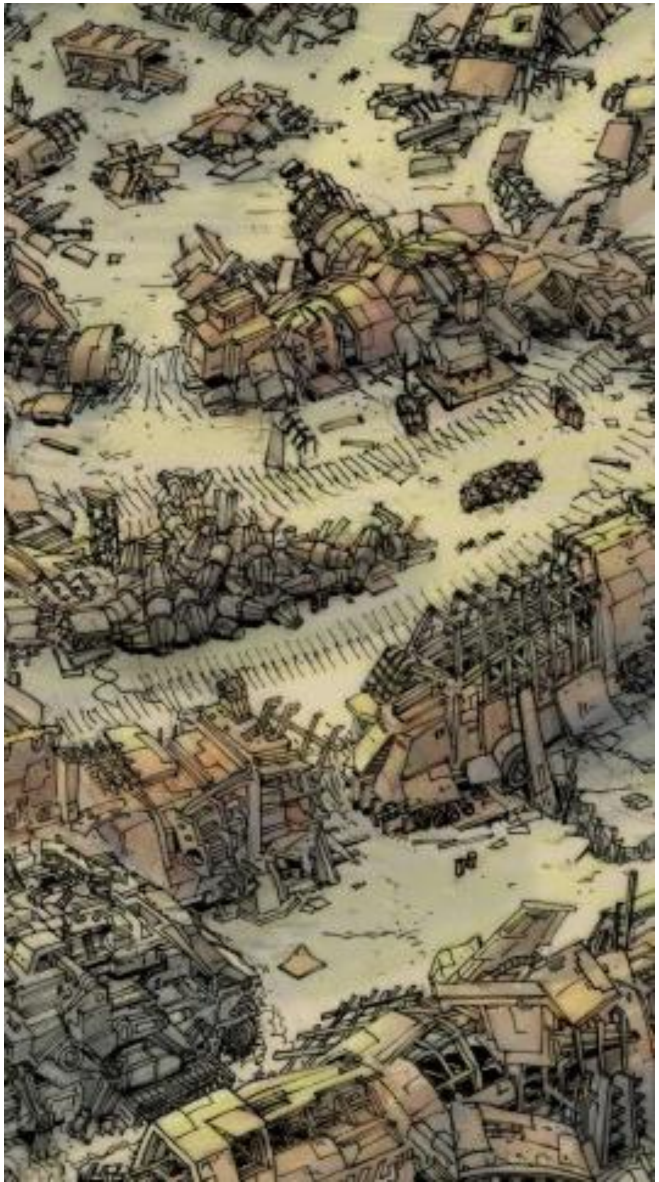
- Tick the boxes here, Jack
- Executive jobs on the line for non-compliance usually means the CISO gets fired
- Some CISOs are just fall guys

Applying for CISO job – 2 questions:

1. What’s my authority
2. What’s my budget

What works: Guerrilla tactics

- Guerrilla's achieve their aim while ‘embedded’ in the territory of their opponent
- Are supported by the ‘natives’
- Difficult to root out if well supported
- Use the resources around them to advance their goals



What that means

Join the club!

- Pet projects (aka ‘strategic initiatives’)
- Multi-use security infrastructure
- Incrementally build security in everywhere
- Embed intelligence horizontally and vertically

Six Security Services

Secure by design	(i) Strategy (ii) Policy and (iii) Architecture
Secure in deployment	(iv) Testing and remediation
Secure in operation	(v) Monitoring and Alerting
Secure in breach	(vi) Incident Response

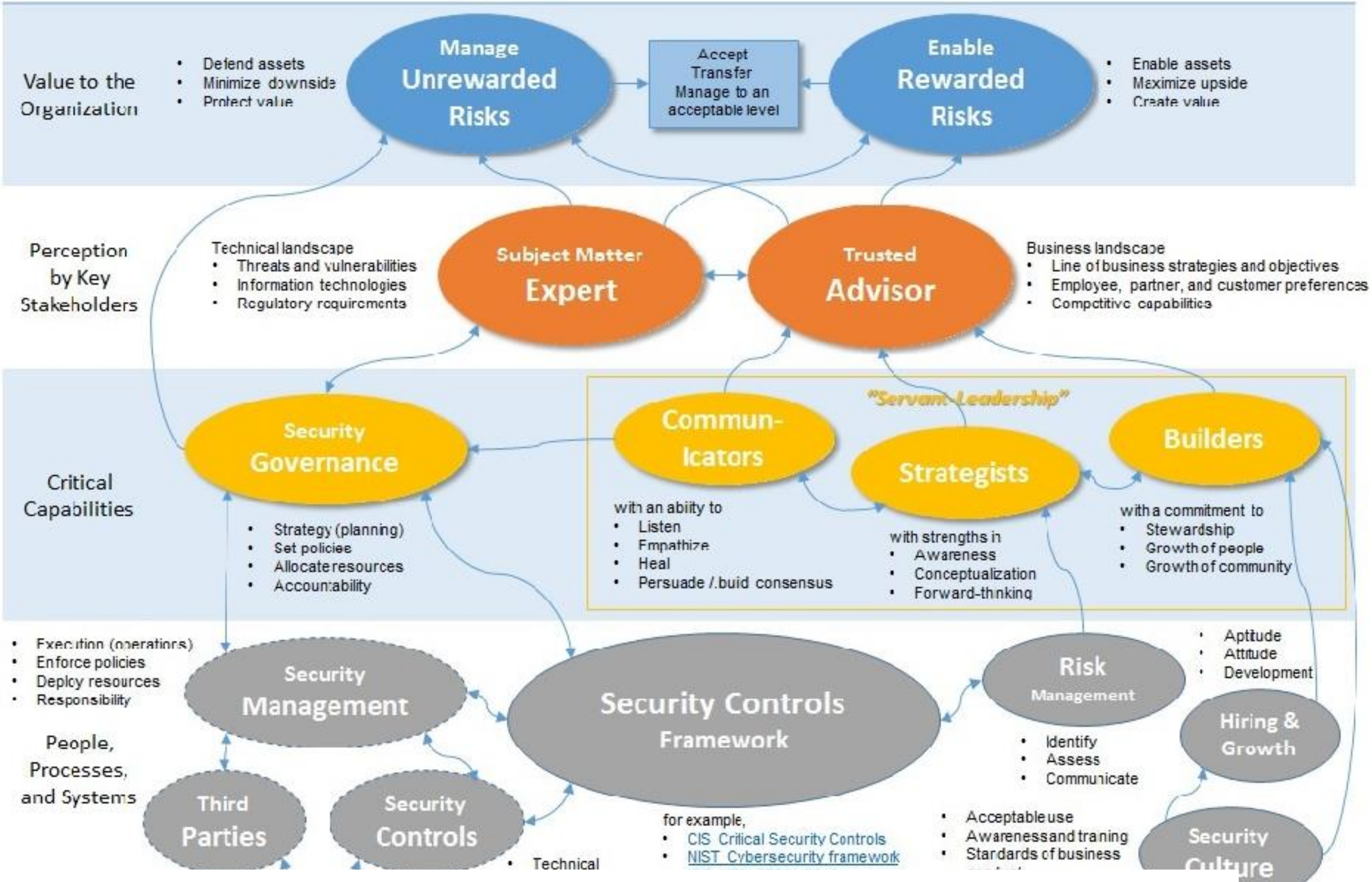
Fuse strategy with tactics

Know where you want to go – i.e. architecture

Know what you want to win and what you can afford to lose

A Strategy Map for Security Leaders

Derek Brink
v 01/2016



Value to the Organization

- Defend assets
- Minimize downside
- Protect value

Manage Unrewarded Risks

Accept
Transfer
Manage to an acceptable level

Enable Rewarded Risks

- Enable assets
- Maximize upside
- Create value

Perception by Key Stakeholders

Technical landscape
- Threats and vulnerabilities
- Information technologies
- Regulatory requirements

Subject Matter Expert

Trusted Advisor

Business landscape
- Line of business strategies and objectives
- Employee, partner, and customer preferences
- Competitive capabilities

Critical Capabilities

Security Governance

- Strategy (planning)
- Set policies
- Allocate resources
- Accountability

"Servant-Leadership"

Commun-Icators

with an abiity to
- Listen
- Empathize
- Heal
- Persuade /.buid consensus

Strategists

with strengths in
- Awareness
- Conceptualization
- Forward-thinking

Builders

with a commitment to
- Stewardship
- Growth of people
- Growth of community

People, Processes, and Systems

- Execution (operations)
- Enforce policies
- Deploy resources
- Responsibility

Security Management

Security Controls Framework

for example,
- CIS Critical Security Controls
- NIST Cybersecurity framework

Risk Management

- Identify
- Assess
- Communicate

- Aptitude
- Attitude
- Development

Hiring & Growth

Third Parties

Security Controls

- Technical

- Acceptable use
- Awareness and traning
- Standards of business

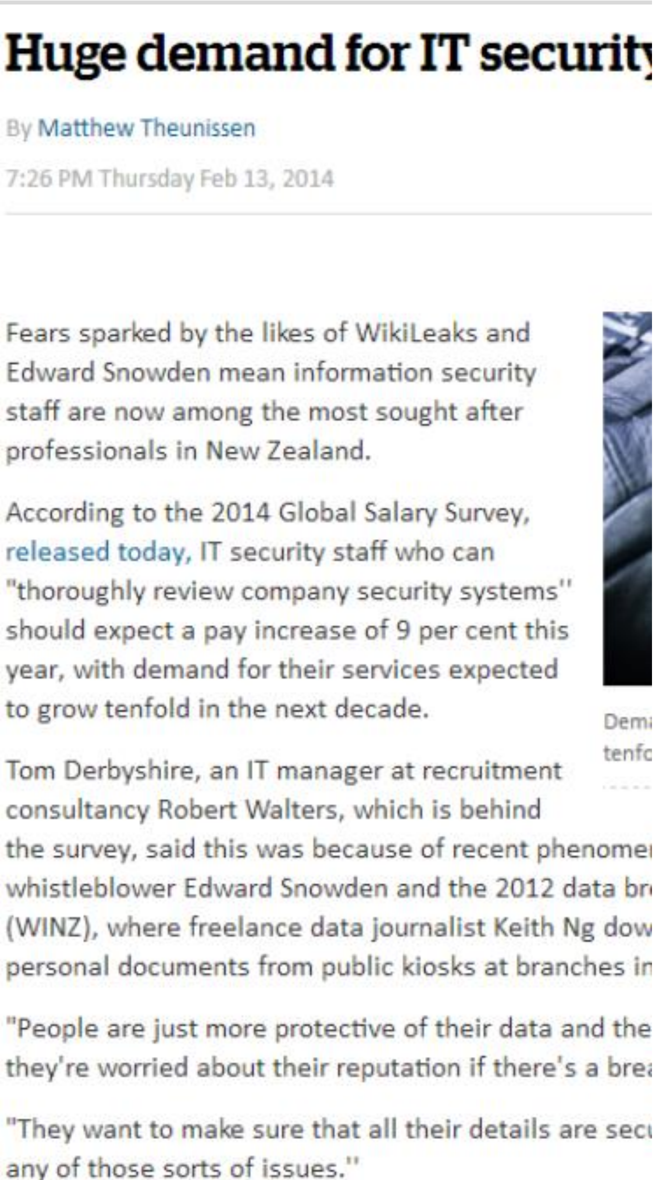
Security Culture

© https://securityintelligence.com/a-strategy-map-for-security-leaders-applying-the-balanced-scorecard-framework-to-information-security/

Building the Team

Staff? It's complicated

Among the professionals most sought after will be […] IT security staff who can thoroughly review company security systems ahead of high profile events. In fact, the demand for IT security specialists is expected to grow tenfold in the next decade." (Robert Walters, Global Salary Survey, Feb 2014, p 280)



Huge demand for IT securit

By Matthew Theunissen

7:26 PM Thursday Feb 13, 2014

Fears sparked by the likes of WikiLeaks and Edward Snowden mean information security staff are now among the most sought after professionals in New Zealand.

According to the 2014 Global Salary Survey, released today, IT security staff who can "thoroughly review company security systems" should expect a pay increase of 9 per cent this year, with demand for their services expected to grow tenfold in the next decade.

Dem
tenfo

Tom Derbyshire, an IT manager at recruitment consultancy Robert Walters, which is behind the survey, said this was because of recent phenome
whistleblower Edward Snowden and the 2012 data br
(WINZ), where freelance data journalist Keith Ng dow
personal documents from public kiosks at branches in

"People are just more protective of their data and the
they're worried about their reputation if there's a brea

"They want to make sure that all their details are secu
any of those sorts of issues."

Work high quality

People like to join high performing groups

Our principles

Enabling: security helps getting better solutions to everyday problems

Transparent: we don’t do many no’s

Blameless: we’re only after hackers, not after users or administrators

Culture - Hiring

Security is a people problem as much as a technical problem

- Don’t hire assholes
- Social skills and ability to interact just as important as technical skills
- Cultural fit
- Diversity

Hackers come in two basic models: coders and makers.

© Scene from Jon Schiefer: ALGORITM: The Hacker Movie. Available on https://youtu.be/6qpudAhYhpc?t=593

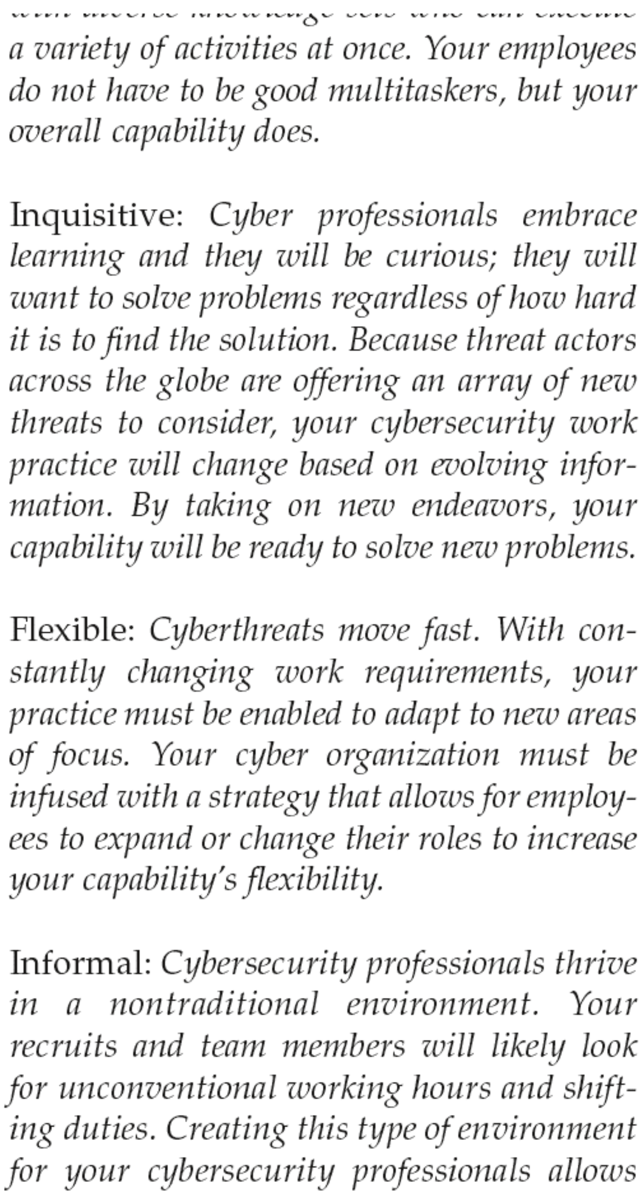
THE UNIVERSITY OF AUCKLAND
Te Whare Wānanga o Tāmaki Makaurau
NEW ZEALAND

Team practices

Think deeply

What are you doing?
What is your team like?
What is the nature and rhythm of the service you provide?
How do you communicate that?

Set up **purpose**



with diverse knowledge sets who can execute a variety of activities at once. Your employees do not have to be good multitaskers, but your overall capability does.

Inquisitive: *Cyber professionals embrace learning and they will be curious; they will want to solve problems regardless of how hard it is to find the solution. Because threat actors across the globe are offering an array of new threats to consider, your cybersecurity work practice will change based on evolving information. By taking on new endeavors, your capability will be ready to solve new problems.*

Flexible: *Cyberthreats move fast. With constantly changing work requirements, your practice must be enabled to adapt to new areas of focus. Your cyber organization must be infused with a strategy that allows for employees to expand or change their roles to increase your capability's flexibility.*

Informal: *Cybersecurity professionals thrive in a nontraditional environment. Your recruits and team members will likely look for unconventional working hours and shifting duties. Creating this type of environment for your cybersecurity professionals allows*

Team Leader!

Two principles

1. The quality of the overall team output is never allowed to drop
2. Everyone in the team grows

Corollaries

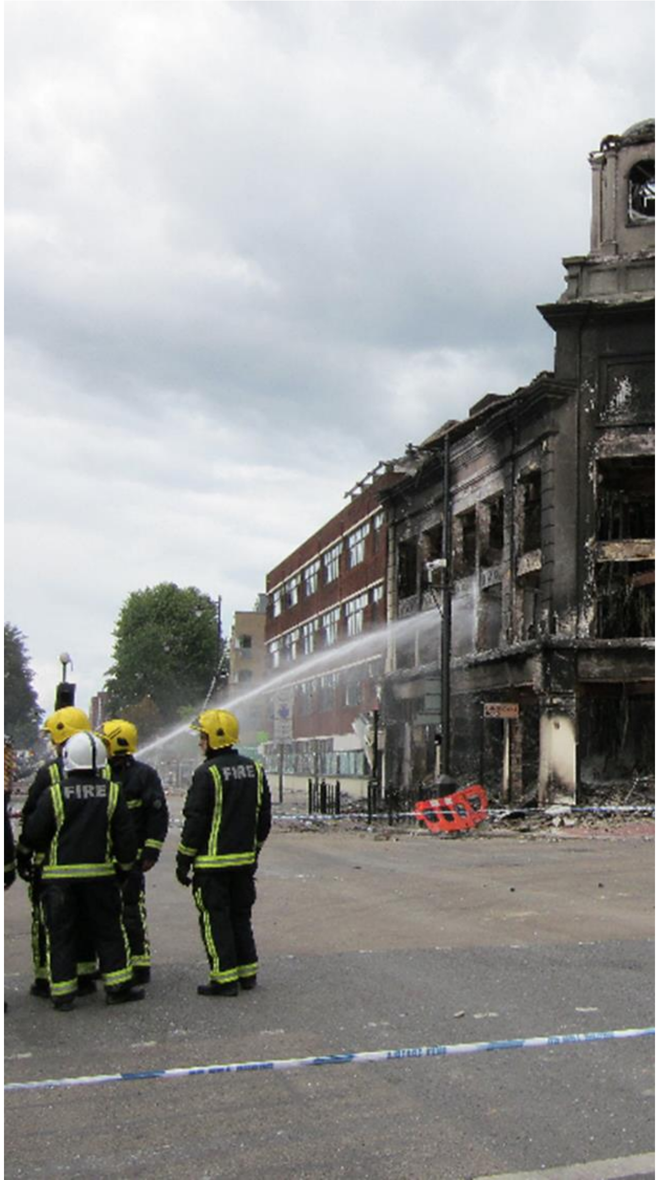
- Everyone has each others' back
- Differences are sorted internally rather than publicly exposed
- Team leader backs team members up to the hilt

Second in command

Team leader should never be a single point of failure

If you’re not there can decisions be made?

5 Team Rules



1. Incidents are a major learning and improvement opportunity
2. Understand the rhythms of security service (daily / monthly / yearly / 5 yearly)
3. Organise a service, rather than put people in jobs
4. Get a second in command who complements you
5. Develop deep trust inside the team

Get your groove on

Play a role in the community - share
Do not spurn vendors (even if you don’t buy from them!)
What industry / tech groups can you team become a member of and contribute to?

Examples

Attack | Defence

Who attacks a University?

People selling access to intellectual property: library and academic documents

People wanting access to services, such as email, publication platforms

Political operations – ‘cyber’ is now part of hybrid war, or the three warfares (psychological, lawfare and media warfare)

Intelligence operations – ‘spying’

[Redacted]

8 slides showing information relating to cyber attacks

THE UNIVERSITY OF AUCKLAND
Te Whare Wānanga o Tāmaki Makaurau
NEW ZEALAND

Some references

http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

https://securityintelligence.com/a-strategy-map-for-security-leaders-applying-the-balanced-scorecard-framework-to-information-security/

www.securityroundtable.org