servicenow

The modern CISO mindset

Shifting from accountability to action

Ben de Bont
Chief Information Security Officer, ServiceNow

Are government frameworks reducing cyber risk?

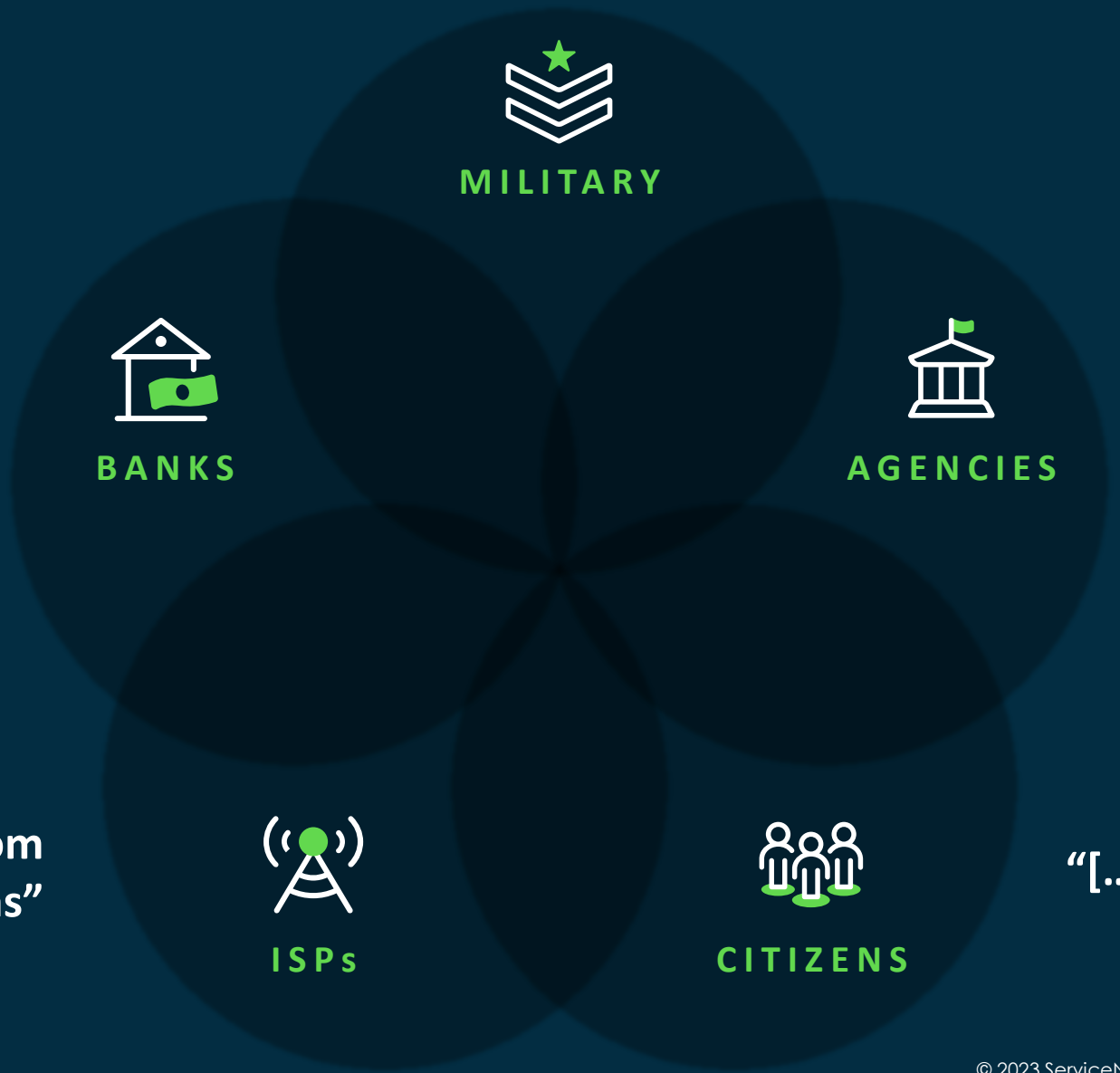
Canadian Cyber Security

- **Privacy Act – (1983)**
- **Personal Information Protection and Electronic Documents Act (PIPEDA) – (2001)**
- **Digital Privacy Act – (2018)**
- **Bill C-26: An Act respecting cyber security, amending the Telecommunications Act – (currently tabled in House of Commons)**
- **Bill C-27 : Digital Charter Implementation Act – (currently tabled in House of Commons)**
- **National Cyber Security Strategy – (In effect since 2010)**
- **National Strategy for Critical Infrastructure (NSCI) – (In effect since 2009)**

Notable ServiceNow global certifications

- **US** – DOD Impact Level 5 (IL5)
- **Singapore** – Multi-Tier Cloud Security (MTCS)
- **Japan** – Information System Security Management & Assessment Program (ISMAP)
- **Germany** – Cloud Computing Compliance Controls Catalog (C5)
- **Korea** – Personal Information Protection Act (PIPA)
- **France** – Health Data Hosting (HDS)
- **UK** – G-Cloud
- **EU** – General Data Protection Regulation (GDPR)

“BLOW UP THE HACKERS”



“We need to satisfy the regulators”

“Jurisdiction of cyber responsibilities”

“Remove users from security decisions”

“[…crickets…]”

US Cyber Security Executive Order

December 2020	March 2021	May 2021	May 2022
SolarWinds	**Microsoft**	**Colonial Pipeline**	**Attestation**
Malicious code discovered in Orion software (Russia)	Announced four zero-days in Exchange; cyber threat actors exploit 250,000 servers	Ransomware attack against company that provides gasoline and jet fuel to Southeastern US (Darkside)	Service providers must attest to all requirement, including:

US EO #14028 rushed into law for all gov agencies, suppliers, and providers

- MFA
- Zero Trust
- Advanced logging & monitoring
- Public/private vulnerability sharing
- Endpoint protection
- Encryption

US Regulation by Enforcement

DOJ Trends

- Holding contractors liable for security failings under the False Claims Act
- Scrutinizing management's role in corporate compliance programs
- Requiring individual accountability for corporate wrongdoing

FTC Trends

- Imposing civil liability on senior executives
- Faulting companies for untimely disclosures or inadequate policies

SEC Trends

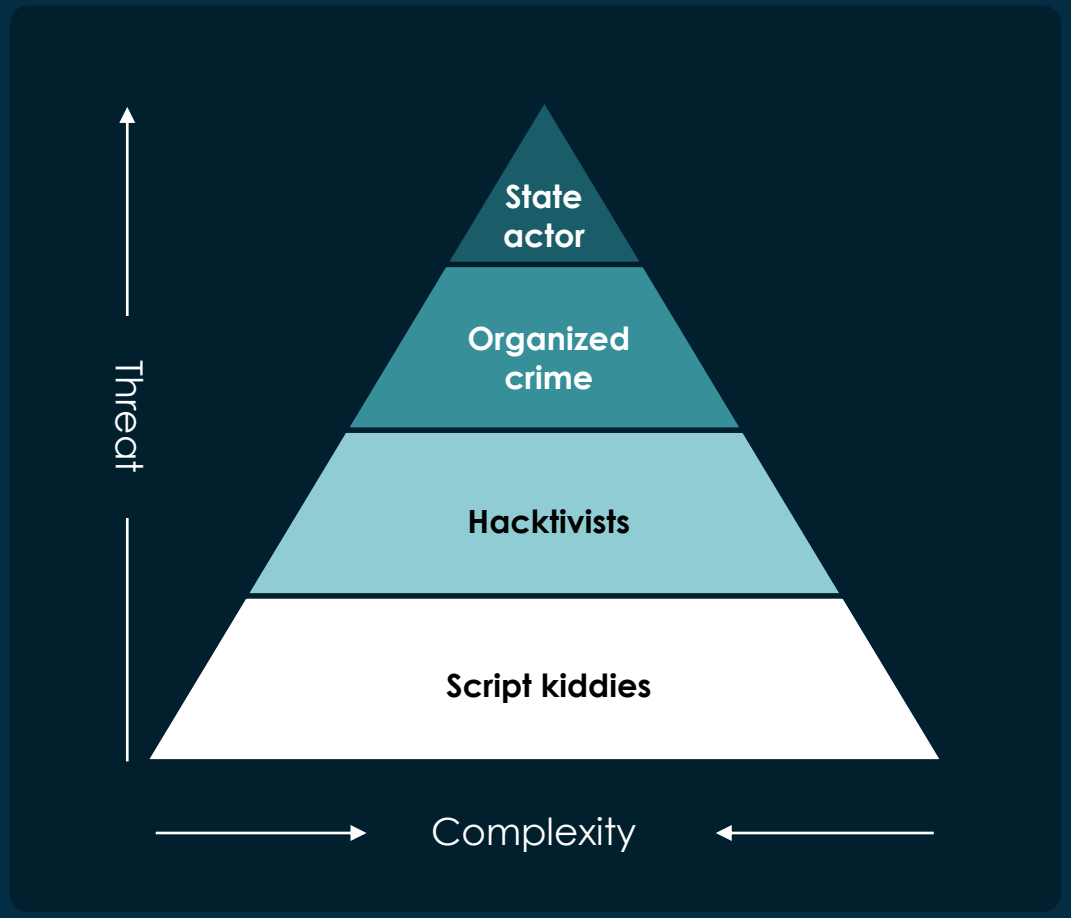
- Fining companies that inadequately protect personal information

Heightened Disclosure Obligations

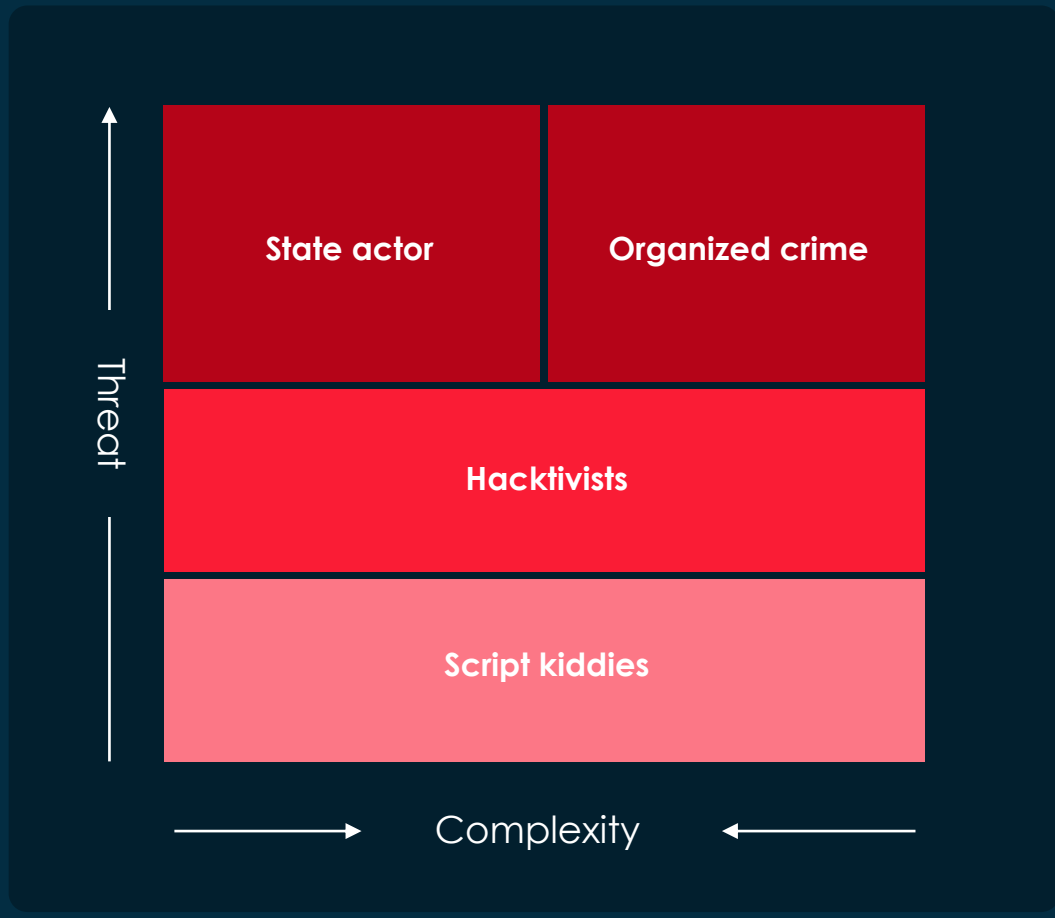
	Regulation	Timeline
Canada	**PIPEDA**	→ **As soon as feasible**
United States	**SEC Item 1.05**	→ **4 business days** to disclose material incidents
	Cyber Incident Response Critical Infrastructure Act	→ **3 business days** to disclose covered cyber incidents
European Union	**Network and Information Security Directive 2**	→ **24 hours** to provide "early warning" after becoming aware of significant incidents
	Cyber Resilience Act	→ **24 hours** to disclose actively exploited vulnerabilities or incidents impacting security
Australia	**Department of Defence - Defence Security Principles Framework**	→ **As soon as possible within 24 hours** of discovering a cyber security incident
India	**Cert-IN Directive issued as part of IT Act**	→ **Within 6 hours**

Would any of these frameworks have stopped the Okta breach?

Cyber security pyramid of pain is now the Cube of Death



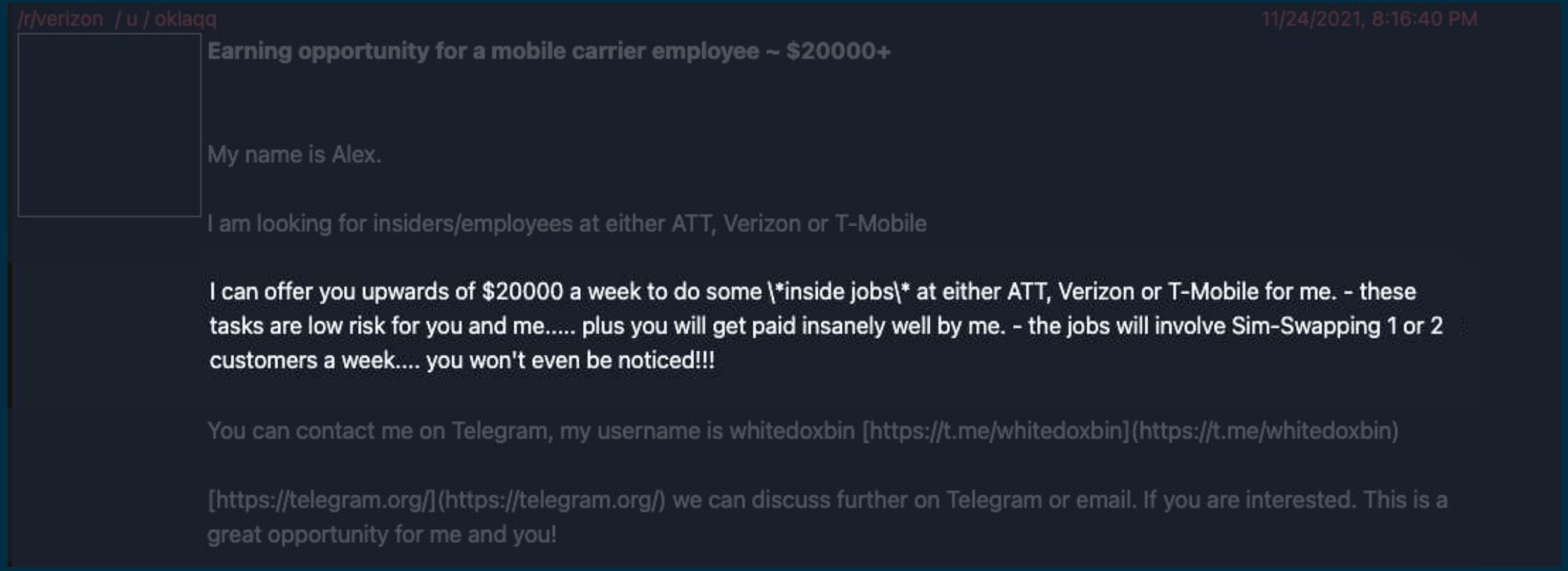
Previous



Now

Low tech…high impact

Lapsus$ “call for participants” demonstrates the barrier of entry is much lower



/r/verizon / u / oklaqq 11/24/2021, 8:16:40 PM

Earning opportunity for a mobile carrier employee ~ $20000+

My name is Alex.

I am looking for insiders/employees at either ATT, Verizon or T-Mobile

I can offer you upwards of $20000 a week to do some *inside jobs* at either ATT, Verizon or T-Mobile for me. - these tasks are low risk for you and me..... plus you will get paid insanely well by me. - the jobs will involve Sim-Swapping 1 or 2 customers a week.... you won't even be noticed!!!

You can contact me on Telegram, my username is whitedoxbin https://t.me/whitedoxbin

https://telegram.org/ we can discuss further on Telegram or email. If you are interested. This is a great opportunity for me and you!

5 Practical CISO Tips to augment your security frameworks

servicenow

5 Practical CISO Tips to augment your security frameworks

1. Understand your entire scope
2. Tap into your team of experts
3. Run practical security tests
4. Optimize tooling to ensure ROI
5. Collaborate to scale security

5 Practical CISO Tips to augment your security frameworks

1

Understand your entire scope

1. Threat model your company
2. Invest in asset discovery
3. Don't restrict your scope with perceived boundaries

2

Tap into your team of experts

3

Run practical security tests

4

Optimize tooling to ensure ROI

5

Collaborate to scale security

5 Practical CISO Tips to augment your security frameworks

1

Understand your entire scope

1. Threat model your company
2. Invest in asset discovery
3. Don't restrict your scope with perceived boundaries

2

Tap into your team of experts

1. Empower your highly technical talent
2. Let developers show you where the problems are
3. Address your known risks, but ready for the unknown

3

Run practical security tests

4

Optimize tooling to ensure ROI

5

Collaborate to scale security

5 Practical CISO Tips to augment your security frameworks

1

Understand your entire scope

1. Threat model your company
2. Invest in asset discovery
3. Don't restrict your scope with perceived boundaries

2

Tap into your team of experts

1. Empower your highly technical talent
2. Let developers show you where the problems are
3. Address your known risks, but ready for the unknown

3

Run practical security tests

1. Reproduce industry incidents
2. Invest in your red team for high ROI
3. Ensure code security ***and*** quality through a mature SDLC

4

Optimize tooling to ensure ROI

5

Collaborate to scale security

5 Practical CISO Tips to augment your security frameworks

1

Understand your entire scope

1. Threat model your company
2. Invest in asset discovery
3. Don't restrict your scope with perceived boundaries

2

Tap into your team of experts

1. Empower your highly technical talent
2. Let developers show you where the problems are
3. Address your known risks, but ready for the unknown

3

Run practical security tests

1. Reproduce industry incidents
2. Invest in your red team for high ROI
3. Ensure code security ***and*** quality through a mature SDLC

4

Optimize tooling to ensure ROI

1. Focus on your needs, not your vendors'
2. Test the effectiveness of your security products
3. Build what you're good at...then buy

5

Collaborate to scale security

5 Practical CISO Tips to augment your security frameworks

1

Understand your entire scope

1. Threat model your company
2. Invest in asset discovery
3. Don't restrict your scope with perceived boundaries

2

Tap into your team of experts

1. Empower your highly technical talent
2. Let developers show you where the problems are
3. Address your known risks, but ready for the unknown

3

Run practical security tests

1. Reproduce industry incidents
2. Invest in your red team for high ROI
3. Ensure code security ***and*** quality through a mature SDLC

4

Optimize tooling to ensure ROI

1. Focus on your needs, not your vendors'
2. Test the effectiveness of your security products
3. Build what you're good at...then buy

5

Collaborate to scale security

1. Be opportunistic to cultivate relationships
2. Use force multipliers, security champions, bug bounties, and more
3. Explain "why" so your people care

servicenow

5 Practical CISO Tips to augment your security frameworks

1

Understand your entire scope

1. Threat model your company
2. Invest in asset discovery
3. Don't restrict your scope with perceived boundaries

2

Tap into your team of experts

1. Empower your highly technical talent
2. Let developers show you where the problems are
3. Address your known risks, but ready for the unknown

3

Run practical security tests

1. Reproduce industry incidents
2. Invest in your red team for high ROI
3. Ensure code security ***and*** quality through a mature SDLC

4

Optimize tooling to ensure ROI

1. Focus on your needs, not your vendors'
2. Test the effectiveness of your security products
3. Build what you're good at...then buy

5

Collaborate to scale security

1. Be opportunistic to cultivate relationships
2. Use force multipliers, security champions, bug bounties, and more
3. Explain "why" so your people care


servicenow