A First Look at Governments' Enterprise Security Guidance

Kimberly Ruth, Raymond Buernor Obu, Ifeoluwa Shode, Gavin Li, Carrie Gates, Grant Ho, Zakir Durumeric

Stanford University

THE UNIVERSITY OF CHICAGO

FS-ISAC

National Cyber Security Centre

a part of GCHQ

इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND INFORMATION TECHNOLOGY

Bundesamt
für Sicherheit in der
Informationstechnik

NSM

CSA
SINGAPORE

Australian Government

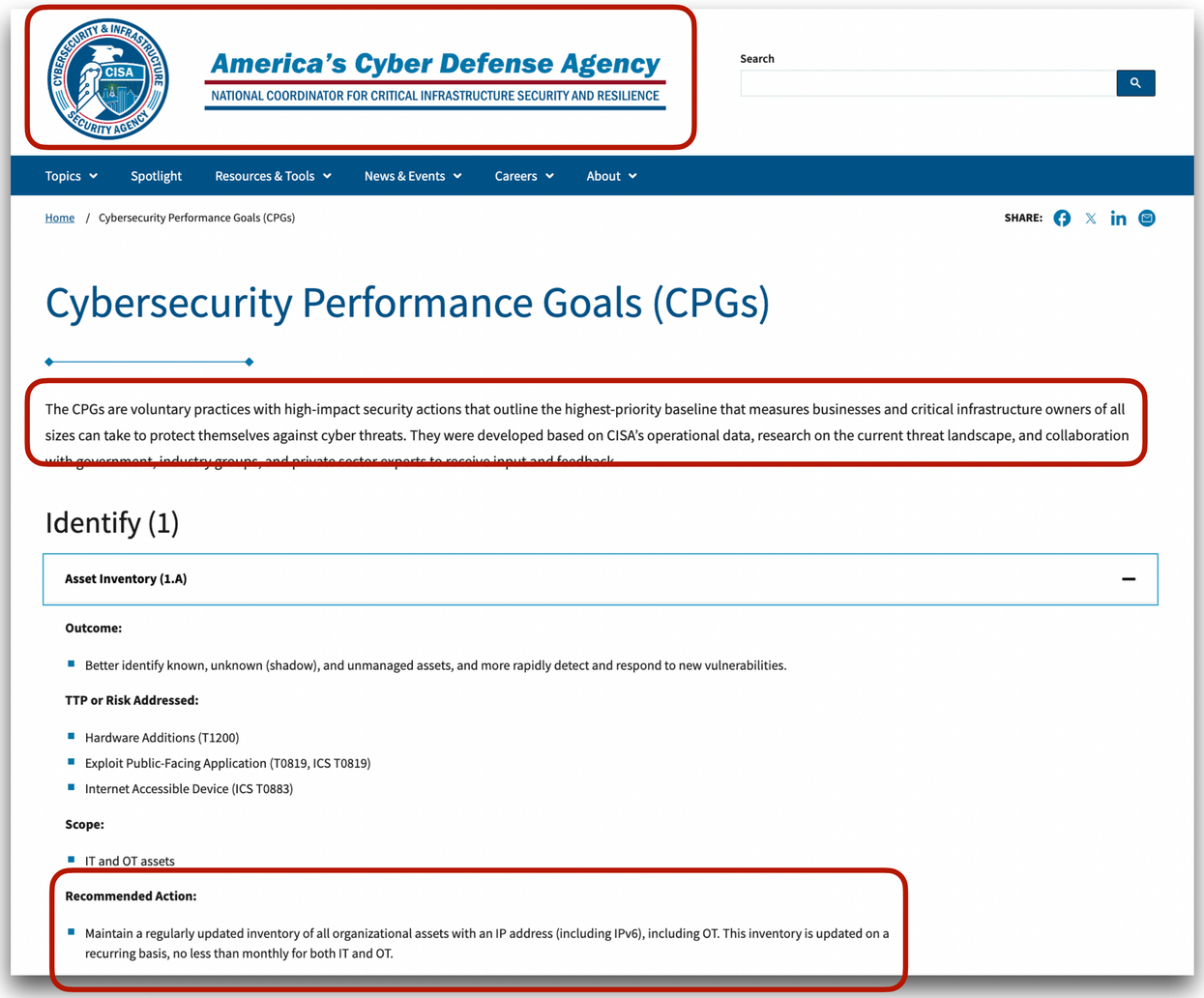
Australian Signals Directorate

Case study: CISA CPGs

US government source

Designed for businesses

List of security controls



What is in this government-authored security guidance for companies?

Research Questions

RQ1: Which governments make **available** security guidance, and how is it scoped and presented?

RQ2: What content is **covered** as essential security guidance for companies, and in what level of depth?

RQ3: How **consistent** are recommended security controls, and do we observe any direct contradictions?

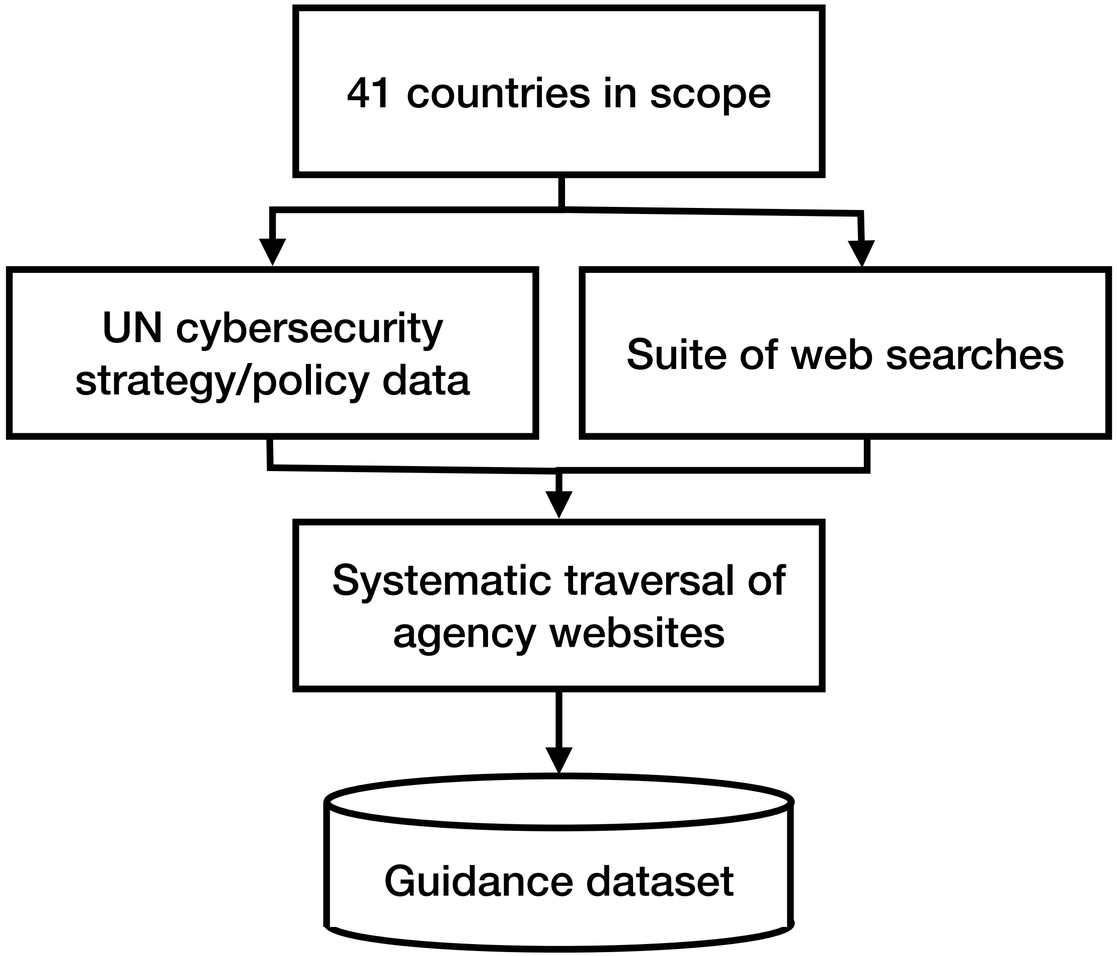
Research Questions

RQ1: Which governments make **available** security guidance, and how is it scoped and presented?

RQ2: What content is **covered** as essential security guidance for companies, and in what level of depth?

RQ3: How **consistent** are recommended security controls, and do we observe any direct contradictions?

Searching for guidance documents



Large volume of government guidance

Every searched country except Russia published resources; many in the dozens

37 / 41 countries publish general-purpose doc; most countries had multiple

US has 18 general-purpose docs from 4 separate agencies; 36 agencies total

The zoo of guidance resources

Audience-Focused	Threat-focused
Sector-specific	Threat model-specific
Size-specific	Mitigation-specific
Technology-specific	Time-sensitive

The zoo of guidance resources

Audience-Focused

Sector-specific

Size-specific

Technology-specific

The zoo of guidance resources

Audience-Focused

Sector-specific

Size-specific

Technology-specific

Government and defense (25)
Telecoms and ISPs (12)

Lawyers (UK)
E-sports (Luxembourg)
Chicken coops (Israel)

The zoo of guidance resources

Government and defense (25)
Telecoms and ISPs (12)

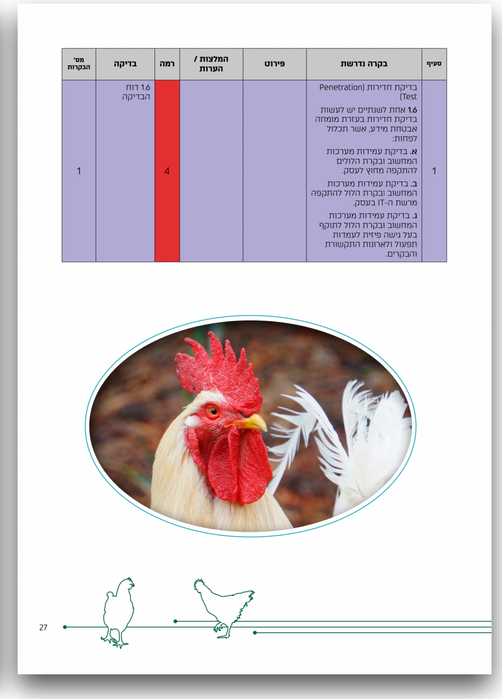
Audience-Focused

Lawyers (UK)
E-sports (Luxembourg)
Chicken coops (Israel)

Sector-specific

Size-specific

Technology-specific



The zoo of guidance resources

Audience-Focused

Sector-specific

Size-specific

Technology-specific

Government and defense (25)
Telecoms and ISPs (12)

Lawyers (UK)
E-sports (Luxembourg)
Chicken coops (Israel)

Mainly SMBs

The zoo of guidance resources

Audience-Focused

Sector-specific

Size-specific

Technology-specific

Government and defense (25)
Telecoms and ISPs (12)

Lawyers (UK)
E-sports (Luxembourg)
Chicken coops (Israel)

Mainly SMBs

Cloud (27)
Network appliances (23)

Dashcams (Malaysia)
Hearing aids (Norway)

The zoo of guidance resources

Threat-focused

Threat model-specific

Mitigation-specific

Time-sensitive

The zoo of guidance resources

(D)DoS (24)
Ransomware (22)

Drone attacks (Spain)
Malicious e-books (Lithuania)

Threat-focused

Threat model-specific

Mitigation-specific

Time-sensitive

The zoo of guidance resources

(D)DoS (24)
Ransomware (22)

Drone attacks (Spain)
Malicious e-books (Lithuania)

Incident response (24)
IAM (24)

Threat-focused

Threat model-specific

Mitigation-specific

Time-sensitive

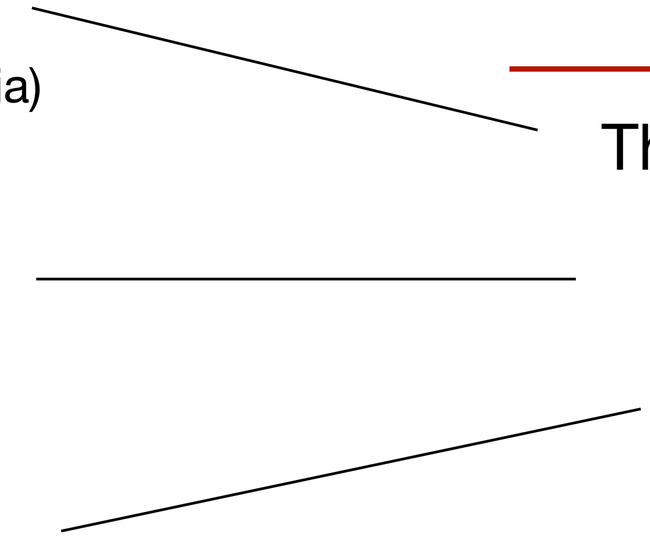
The zoo of guidance resources

(D)DoS (24)
Ransomware (22)

Drone attacks (Spain)
Malicious e-books (Lithuania)

Incident response (24)
IAM (24)

Threat intel and CVEs



Threat-focused

Threat model-specific

Mitigation-specific

Time-sensitive

The zoo of guidance resources

Audience-Focused	Threat-focused
Sector-specific	Threat model-specific
Size-specific	Mitigation-specific
Technology-specific	Time-sensitive

Most countries have most of these types of guidance

Governments publish massive amounts of guidance resources with wildly varying scope and presentation choices.

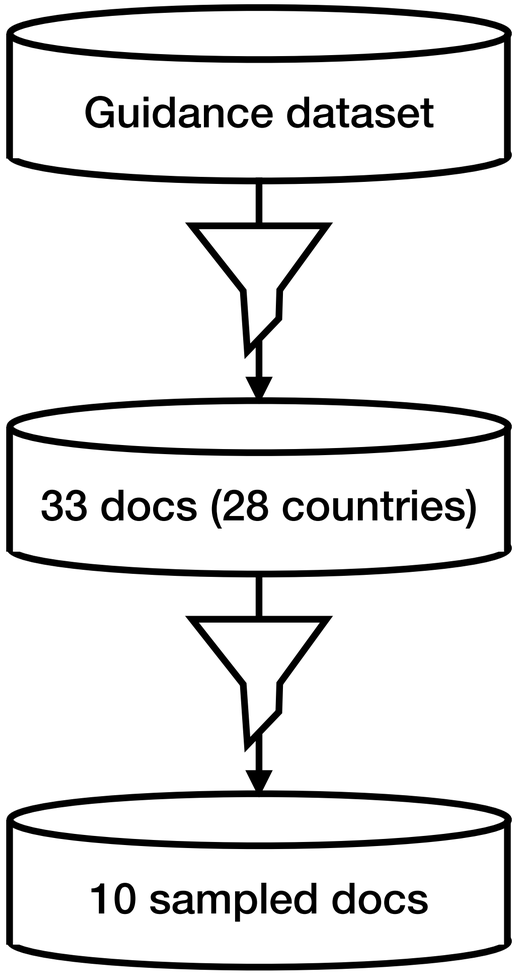
Research Questions

RQ1: Which governments make **available** security guidance, and how is it scoped and presented?

RQ2: What content is **covered** as essential security guidance for companies, and in what level of depth?

RQ3: How **consistent** are recommended security controls, and do we observe any direct contradictions?

Choosing documents for analysis



General-purpose documents
Framed as “essential” controls

Geographically-distributed sample
Spectrum of document lengths

High-priority security interventions
according to governments globally

Building a content analysis framework

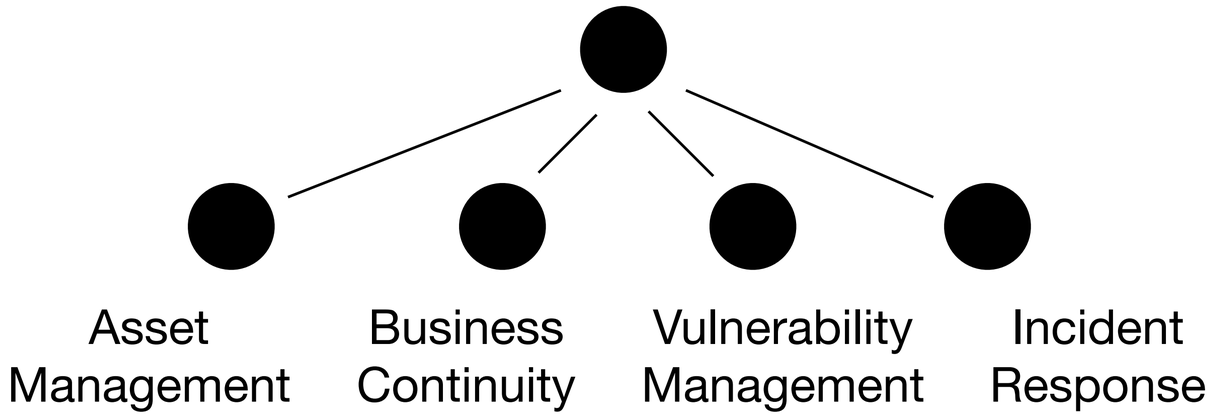
Common controls frameworks: industry-made tools to help companies efficiently demonstrate adherence to popular security standards

Apply qualitative methods to adapt and extend existing frameworks

End product: a reasonably *comprehensive* and *hierarchical* content analysis framework

Taxonomy of guidance content

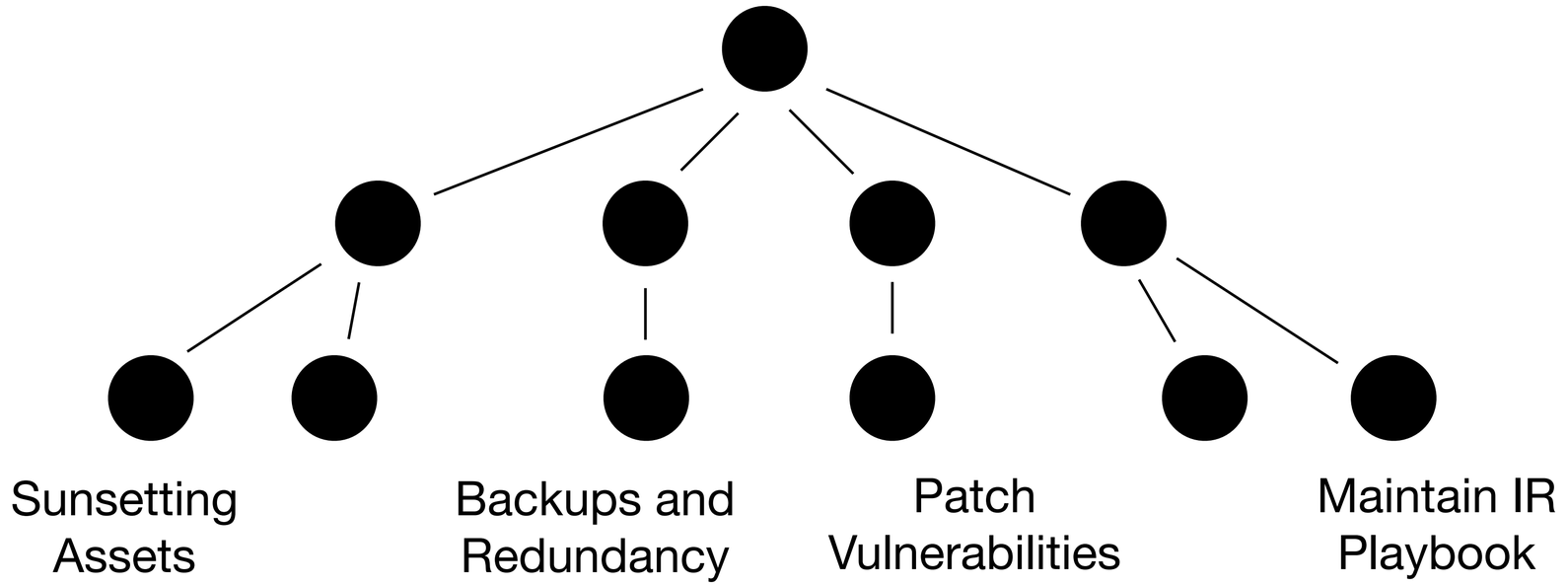
Themes



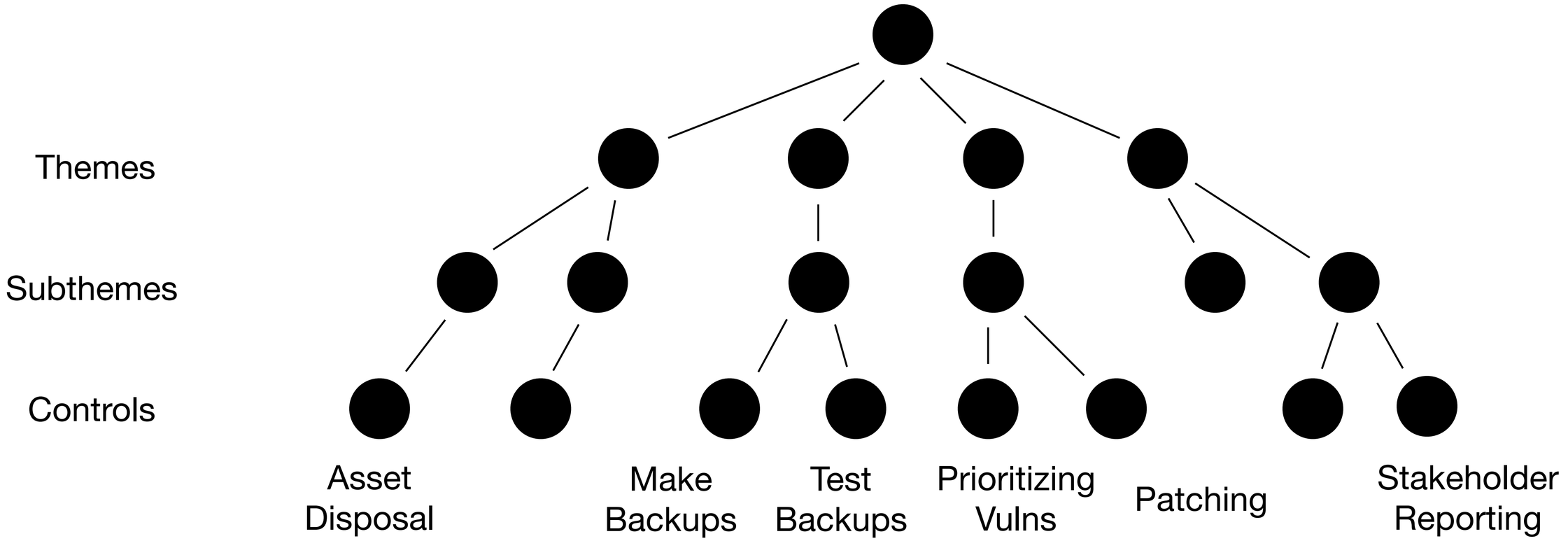
Taxonomy of guidance content

Themes

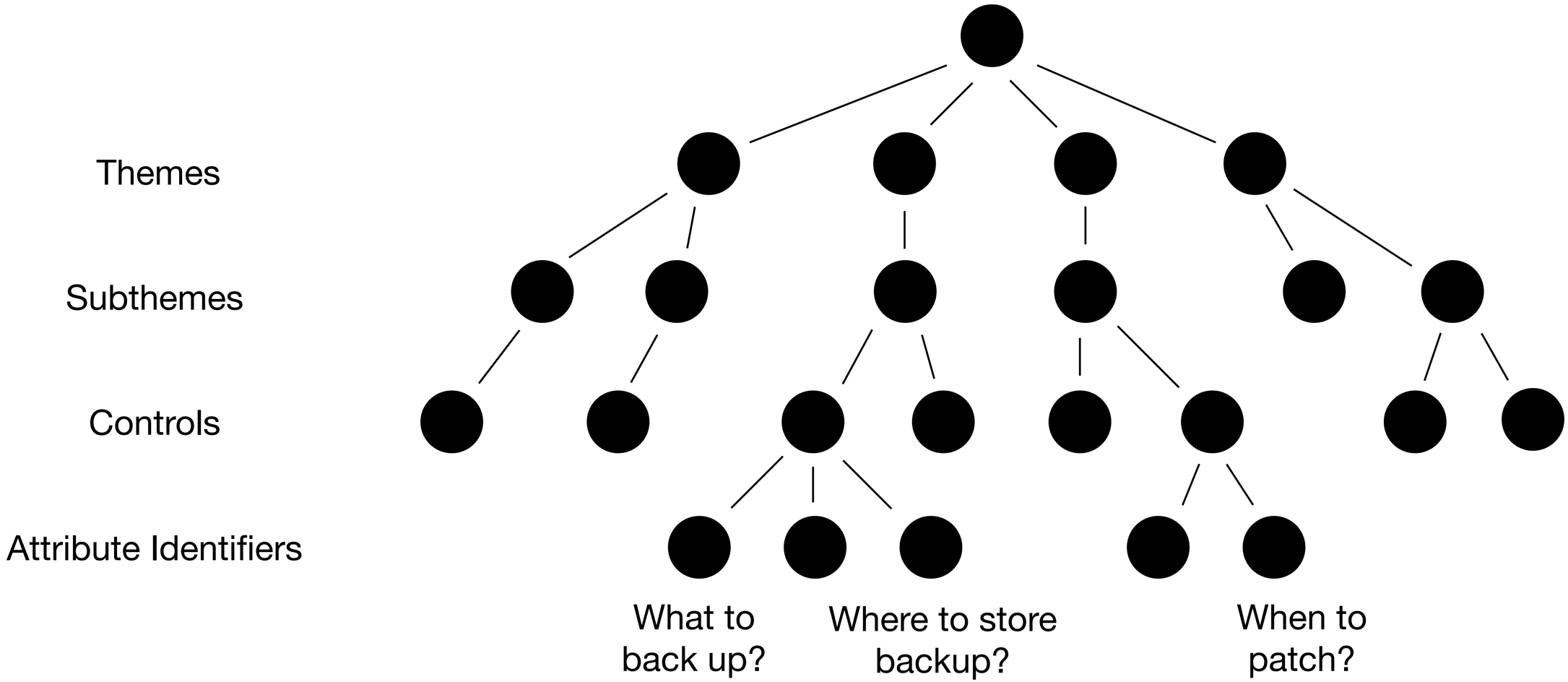
Subthemes



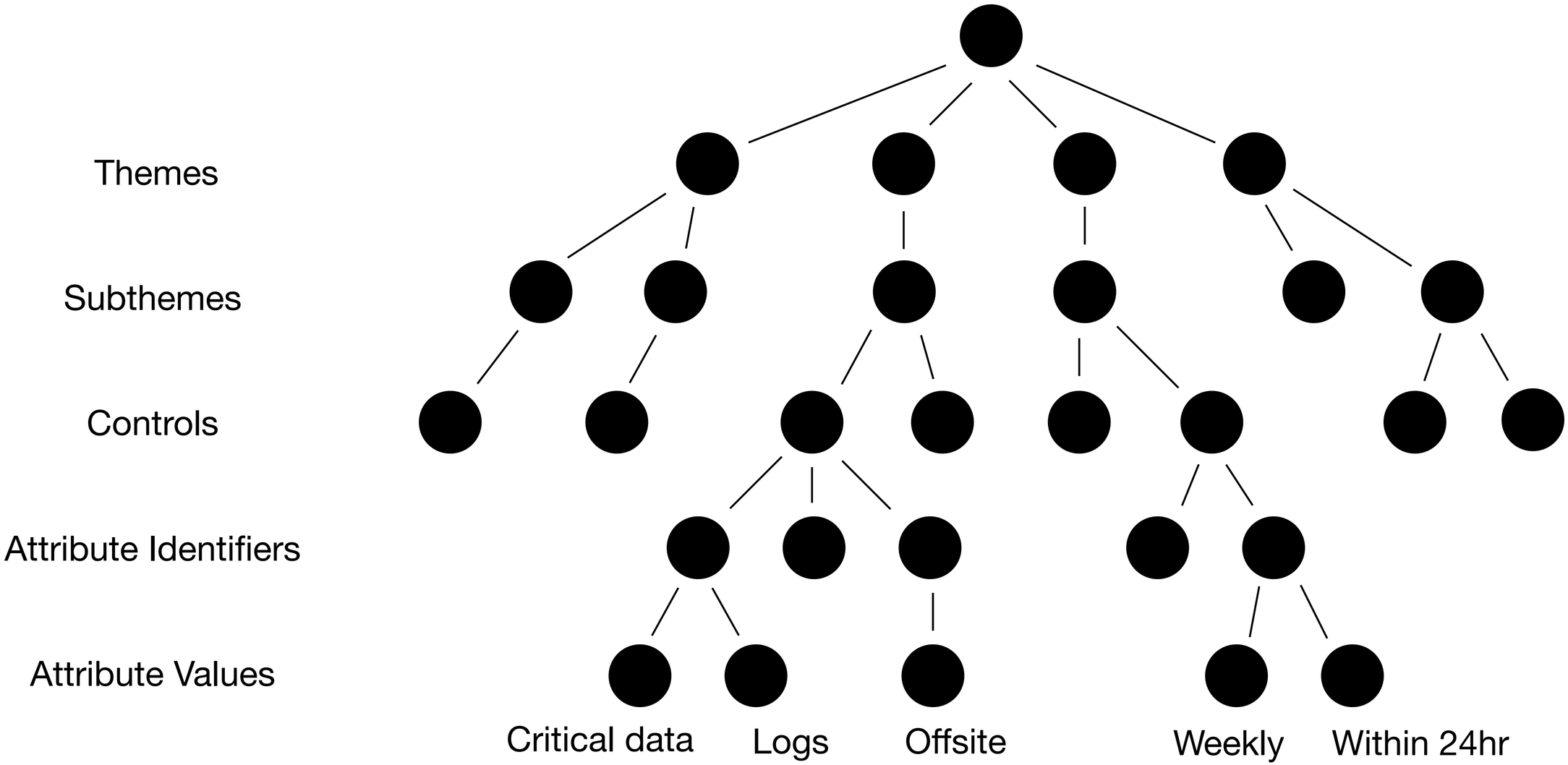
Taxonomy of guidance content



Taxonomy of guidance content



Taxonomy of guidance content



Taxonomy of guidance content

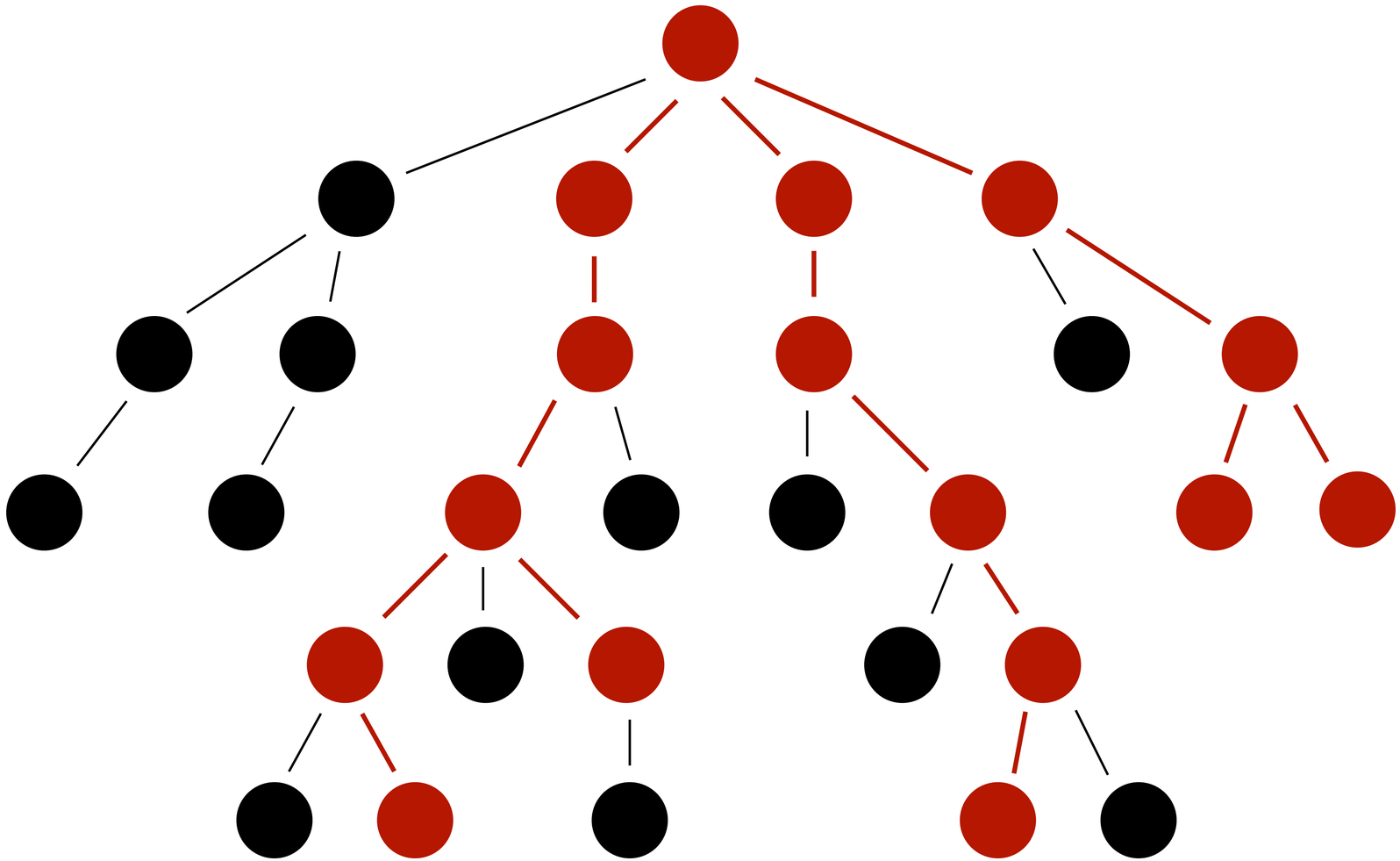
Themes

Subthemes

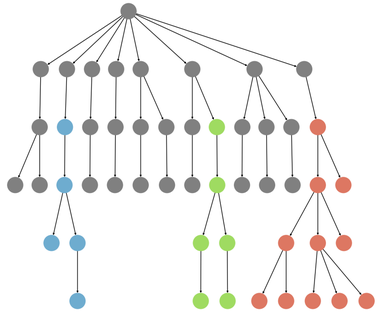
Controls

Attribute Identifiers

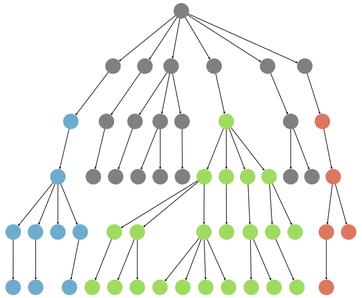
Attribute Values



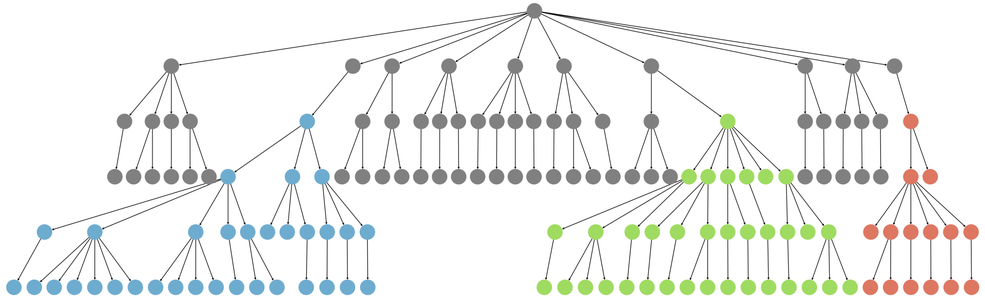
Content varies in breadth and depth



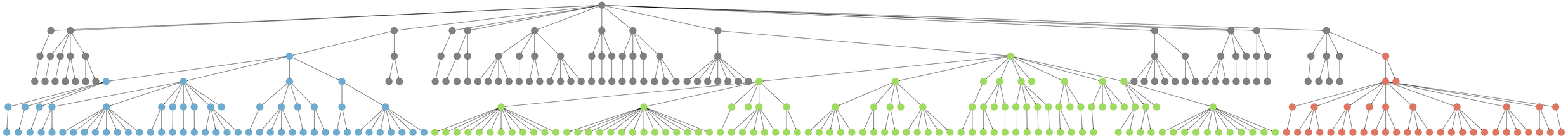
Israel



Ukraine

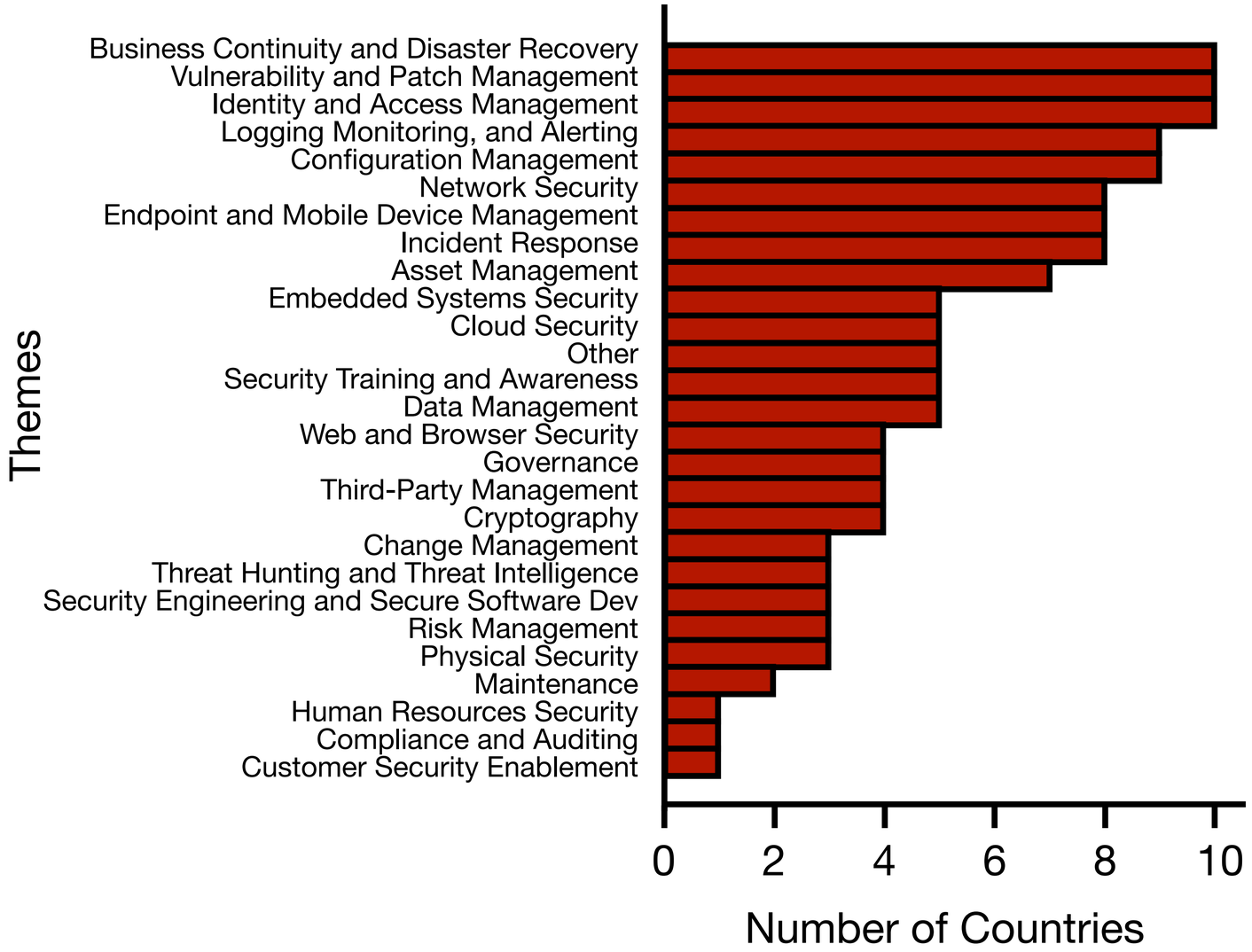


Singapore

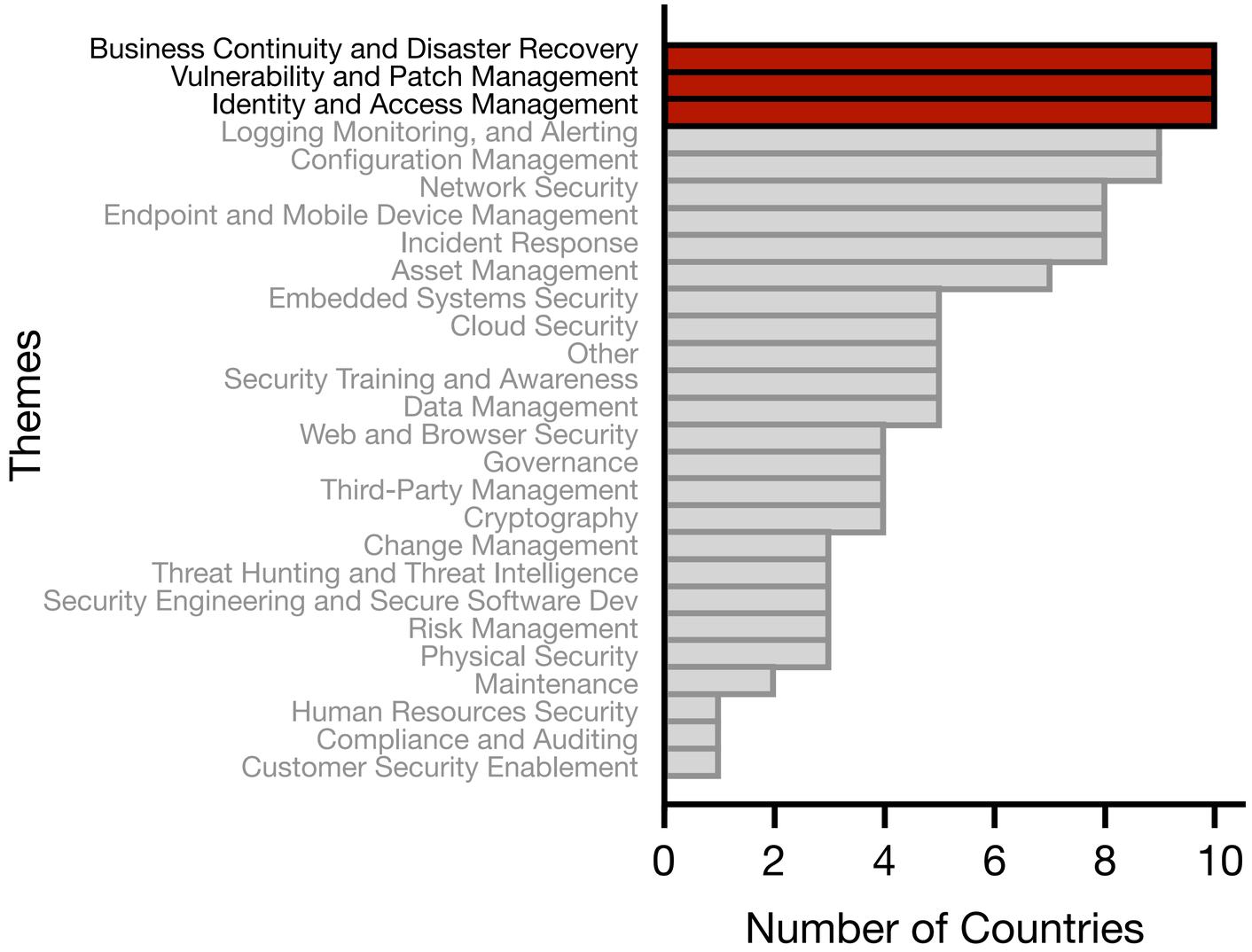


New Zealand

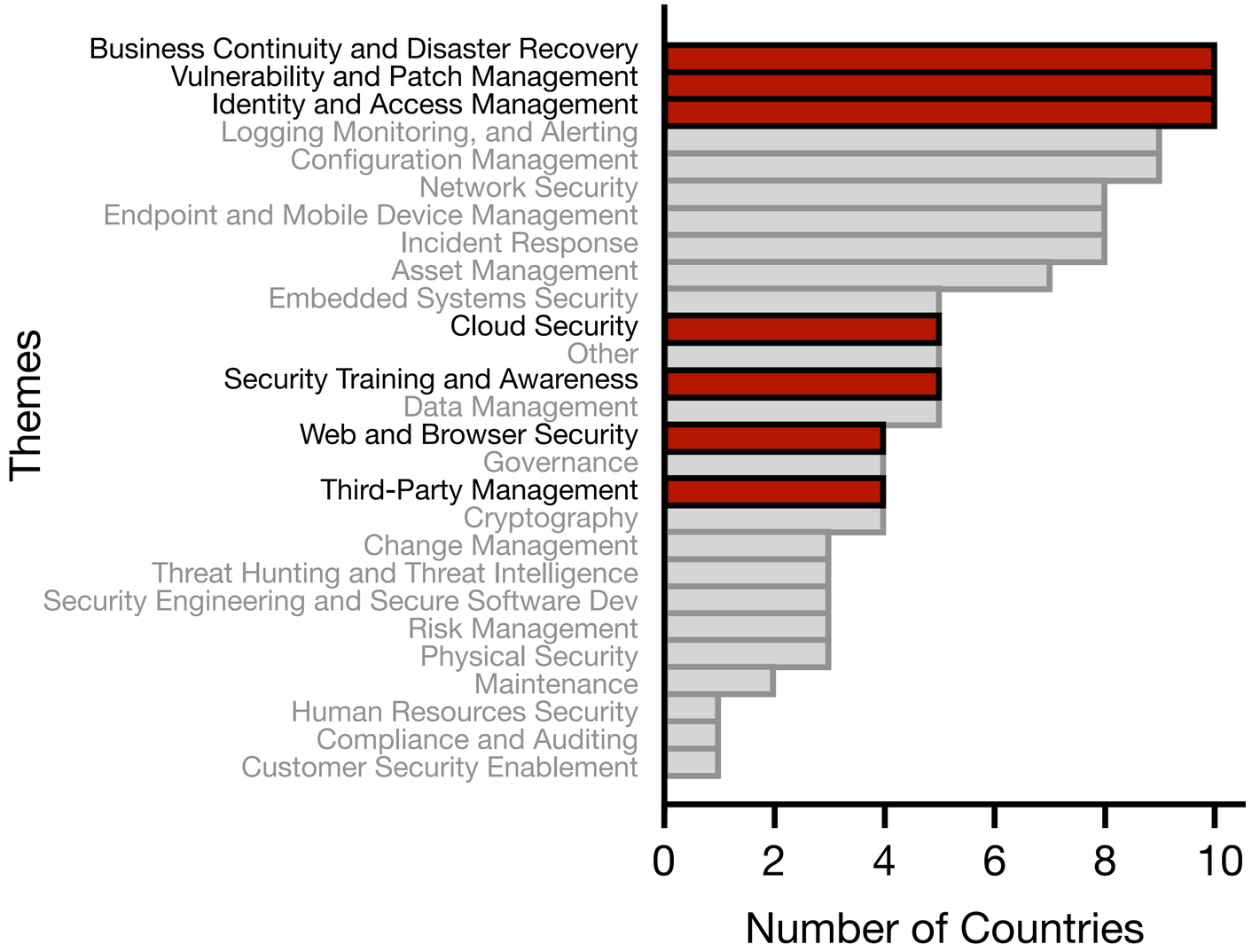
Mixed coverage of most themes



Mixed coverage of most themes



Mixed coverage of most themes



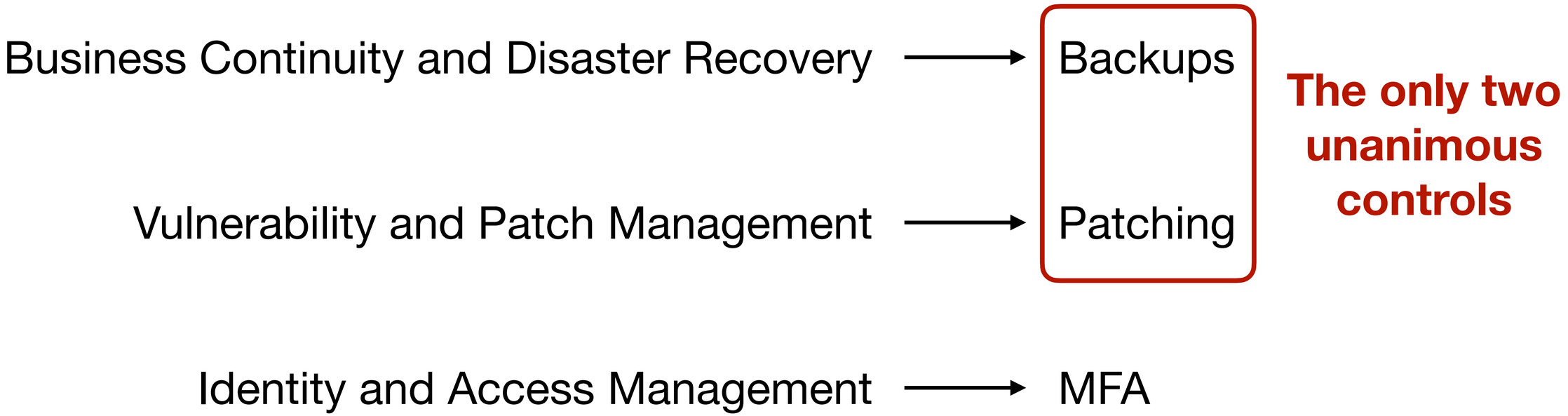
Few unanimous recommendations

Business Continuity and Disaster Recovery ⟶ Backups

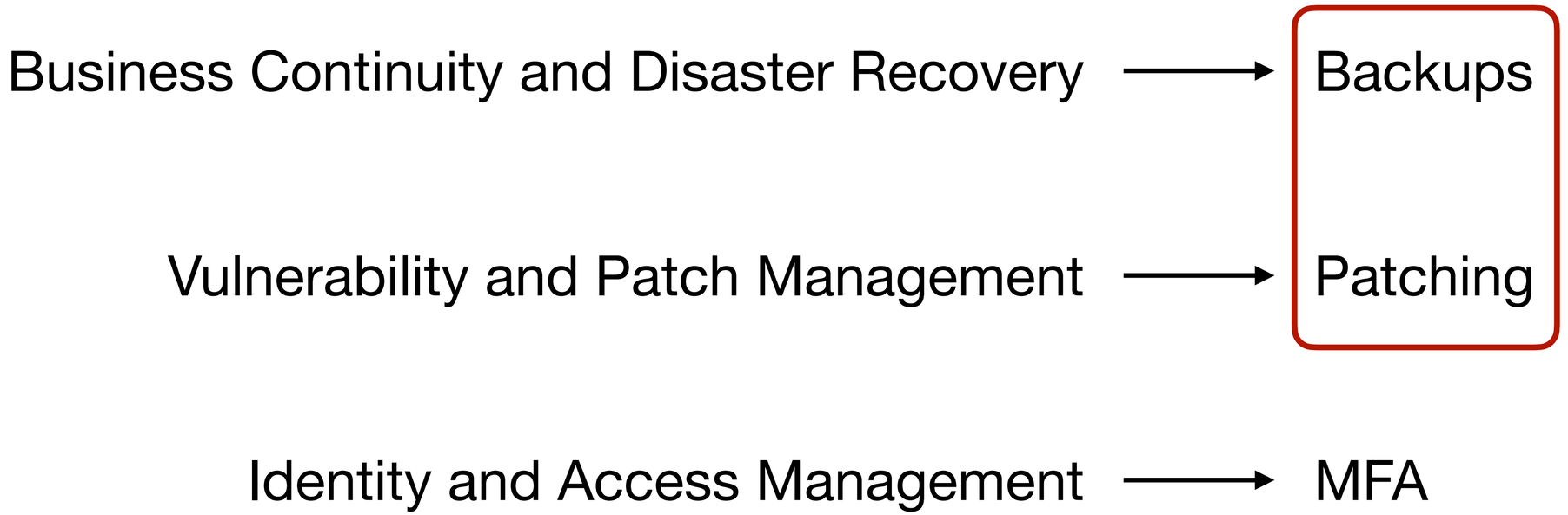
Vulnerability and Patch Management ⟶ Patching

Identity and Access Management ⟶ MFA

Few unanimous recommendations



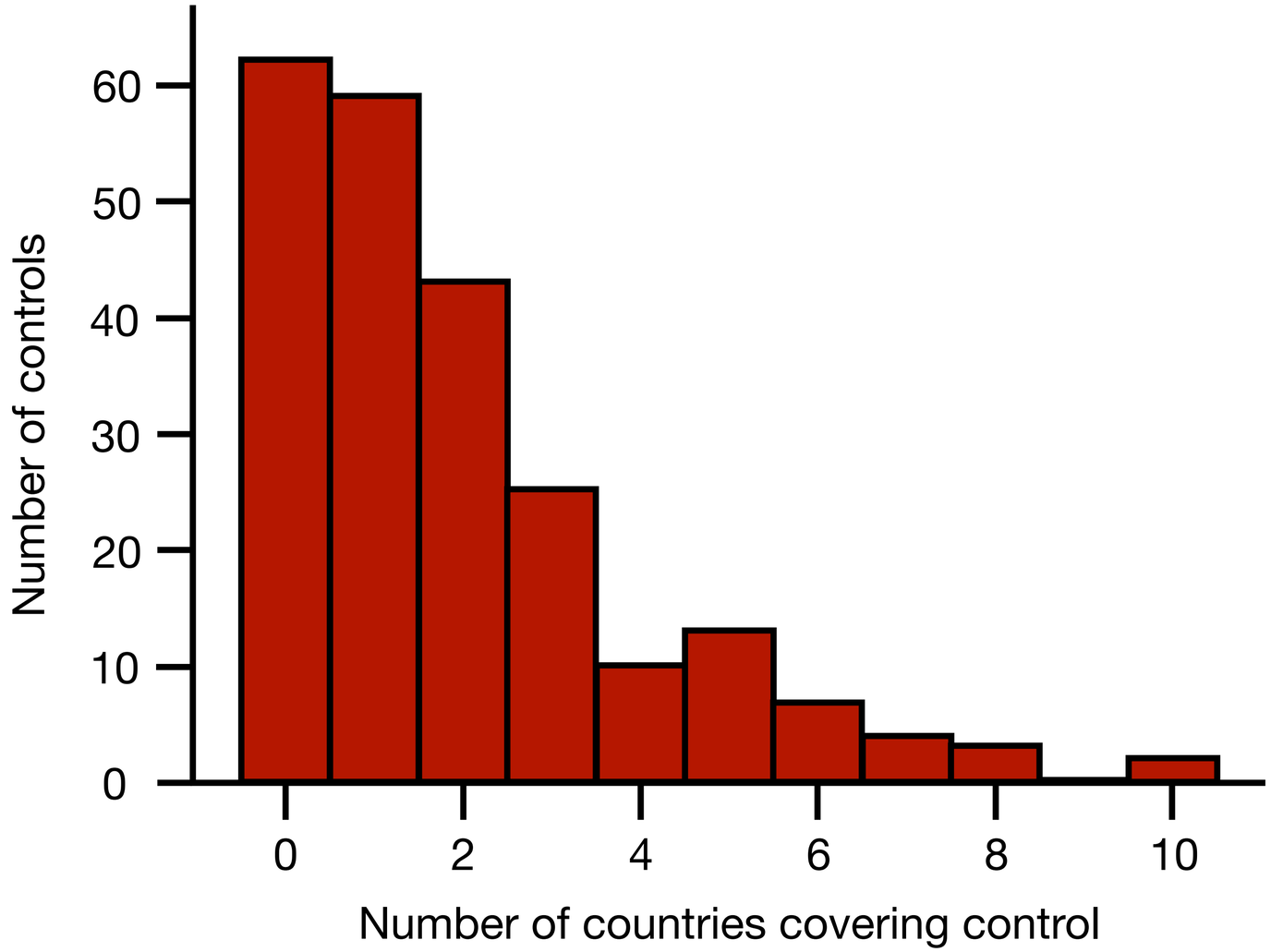
Few unanimous recommendations



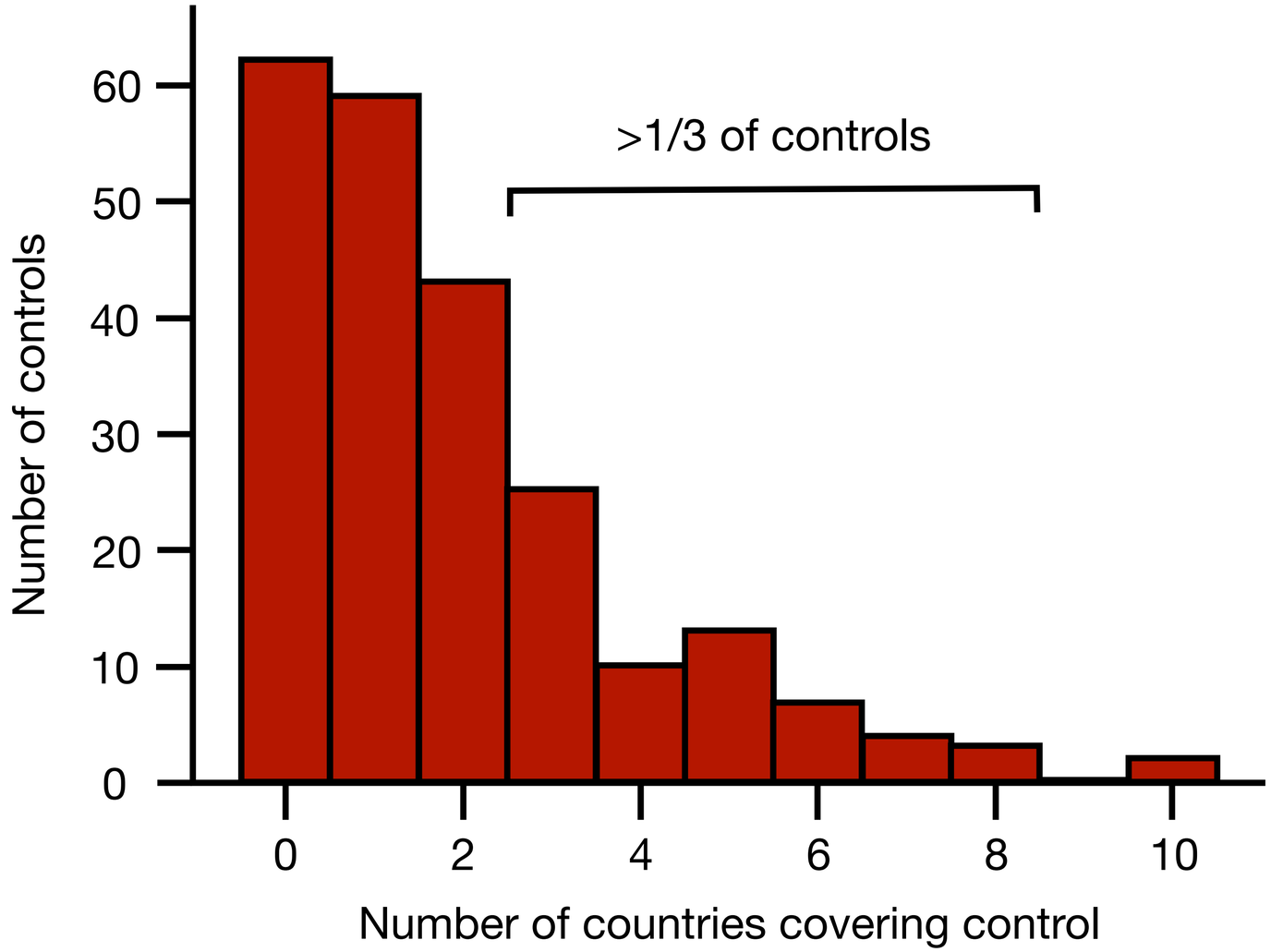
The only two unanimous controls

Only 5 / 166 (3%) of controls are recommended by at least 75% of countries

Little consensus on control inclusion



Little consensus on control inclusion



Rare guidance controls

"Microsoft Office's **list of trusted publishers is validated** on an annual or more frequent basis" — Australia

"Details that are not essential to the functioning of the organization's system **should not be disclosed outside the organization**, unless there is a specific business need" — Israel

"Organizations sponsor at least one **'pizza party'** or equivalent social gathering per year that is focused on strengthening working relationships **between IT and OT security personnel**" — US

Countries differ more than they agree

Most countries differ pairwise by **more than half** their total content

Countries differ more than they agree

Most countries differ pairwise by **more than half** their total content

UK

US

Five Eyes members

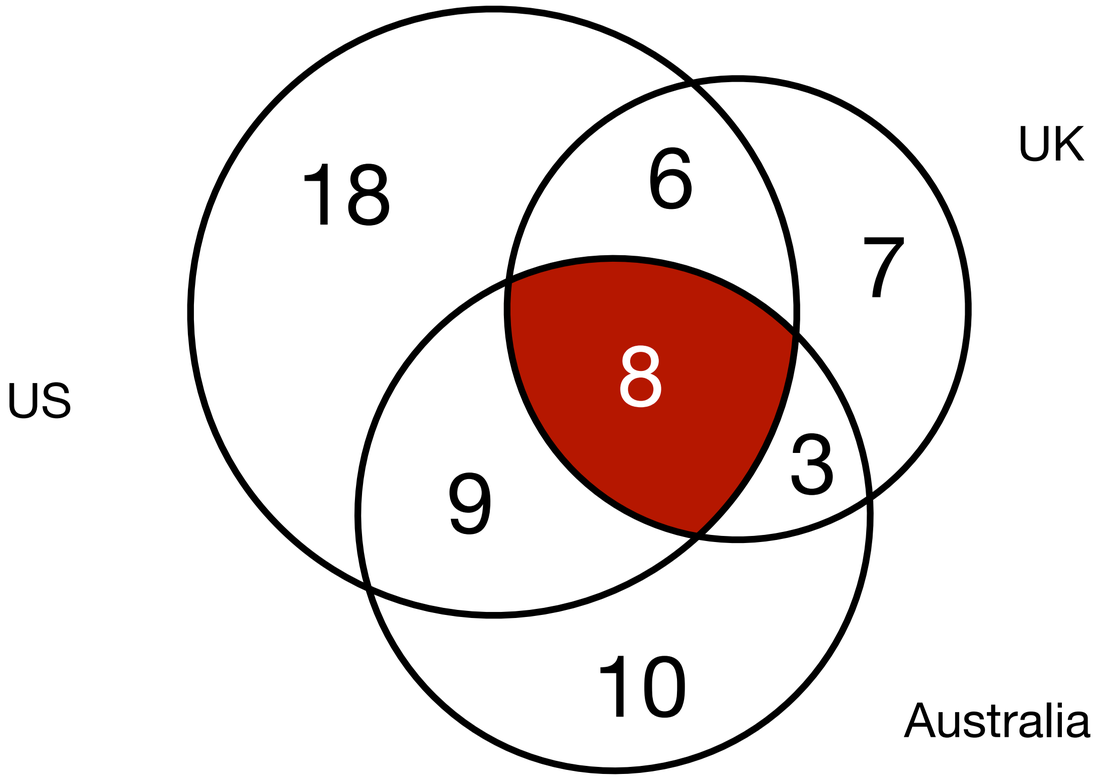
Australia

Countries differ more than they agree

Most countries differ pairwise by **more than half** their total content

Nearly as much **disagreement among close allies**:

only 8 of 61 (**13%**) recommendations in common

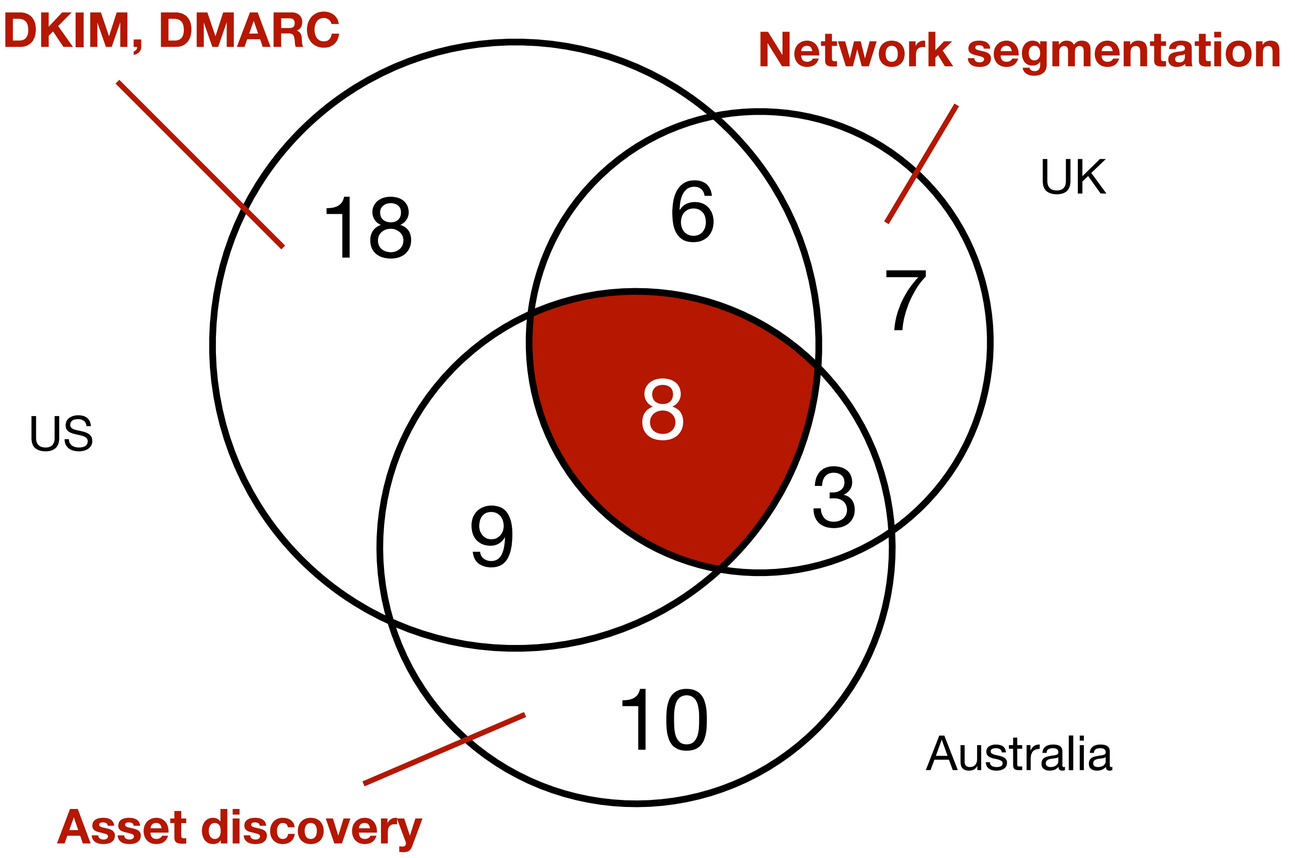


Countries differ more than they agree

Most countries differ pairwise by **more than half** their total content

Nearly as much **disagreement among close allies**:

only 8 of 61 (**13%**) recommendations in common



Countries do not agree on what should constitute “essential” security advice for companies.

Research Questions

RQ1: Which governments make **available** security guidance, and how is it scoped and presented?

RQ2: What content is **covered** as essential security guidance for companies, and in what level of depth?

RQ3: How **consistent** are recommended security controls, and do we observe any direct contradictions?

To specify or not to specify?

"A comprehensive backup of **all assets**" — Israel

"the software used is updated **periodically**" — Egypt

"Stored information […] **includes at a minimum**: configurations, roles, programmable controller (PLC) logic, engineering drawings, and tools" — US

"Patches […] in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied **within two weeks** of release." — Australia

Some have a long tail of unique details

“Backup administrator accounts are prevented from modifying and deleting backups during their retention period” — Australia

“patching […] at a time that will allow the component to be rebooted without massive disruption” — New Zealand

“manual controls must be tested to ensure that critical functions will remain operable” — Egypt

Direct contradictions between advice

"**Only use the latest** version with the latest security functions" — Norway

"The latest release, or the **previous** release" — Australia

"latest **stable** (non-vulnerable) version" — India

"**contain** letters, numbers and special characters" — Ukraine

"**not enforcing** password complexity requirements" — UK

Countries disagree on what details to describe, and sometimes outright contradict each other.

Rethinking enterprise guidance

- Consensus-driven guidance does not result in consistent body of advice
- High-volume and inconsistent guidance places the burden on practitioners
- Need to design security advice in a more principled, evidence-driven way

Thank you!

Takeaways:

- Governments publish voluminous guidance resources with varying scope
- Countries do not agree on “essential” security advice for companies
- Countries’ guidance sometimes outright contradicts each other

Contact:

Kimberly Ruth
kcruth@cs.stanford.edu