WE ARE THE

CompTIA®

Community

CompTIA Community ANZ Regional Meeting

Adelaide 20 September 2024

WE ARE THE CompTIA® Community

WELCOME & INTRODUCTIONS

MJ SHOER, CHIEF COMMUNITY OFFICER, COMPTIA

- **Antitrust**
  You must not engage in discussions that could result in an unreasonable restraint of trade.
  https://www.comptia.org/membership/communities-and-councils/antitrust-statement

- **Diversity**
  We promote an inclusive environment that respects and values all individuals.
  https://comptia.informz.net/COMPTIA/pages/CompTIAATTD

- **Anti-Harassment**
  This is a respectful and safe environment for all. Any verbal, physical, or psychological harassment will not be tolerated. https://www.comptia.org/contact-us/harassment-complaint

ANTITRUST, DIVERSITY & ANTI-HARASSMENT

PLEASE REPORT ANY VIOLATION OF THE ABOVE POLICIES TO COMPTIA STAFF IMMEDIATELY.
VIOLATORS WILL BE REMOVED FROM THE EVENT OR MEETING

WHO IS CompTIA?

CompTIA is the vendor-neutral, non-profit trade association and leading IT certification provider for the industry and its workforce.

The CompTIA Community is the membership arm of CompTIA. We are an IT Channel Community made up of MSPs/Solution Providers, vendors, distributors, and associate member companies from across the globe.

This is all about **YOU!**

WE ARE THE CompTIA® Community

9:15 – 9:45 AM

WELCOME

MJ SHOER, CHIEF COMMUNITY OFFICER, COMPTIA

WE ARE THE CompTIA® Community

EXECUTIVE COUNCIL MEMBERS

Each region is led by an Executive Council of 12 volunteer leaders who represent the interests of the members in the region and bring real-world perspectives to our member-led content and initiatives. You may express your interest at any time. Email: RStamell@CompTIA.org

CompTIA Community Executive Council ANZ

DAVID NORRIS

Chair
Nortec IT (MSP)

MARIA ARMSTRONG

Vice Chair
Pax8 (Distributor)

SCOTT ATKINSON

TribeTech (MSP)
MSP Interest Group Chair

GERARDO BARANQUERO

Avocado (MSP)

DEAN CALVERT

Calvert Technologies/ BlackbirdIT (MSP)

NICK CLIFT

Tenasaia (MSP)

SCOTT GREEN

Aportio (MSP)

WARWICK GREY

Fabric Partners NZ (MSP)
EmTech Interest Group Chair

AARON JACOBS

Sophos (Vendor)

KELLY JOHNSON

Acronis (Vendor)
Cybersecurity Interest Group Chair

KAREEM TAWANSI

Solentive (MSP)

SHAUN WITHERDEN

Kaseya (Vendor)

CompTIA Community Team

CompTIA Community

MJ Shoer

Chief Community Officer

Estelle Johannes

Senior Director, Regional Groups

Wayne Selk

VP, Cybersecurity Programs

Kris Nagamootoo

Senior Director, Member Experience

Rose Stamell

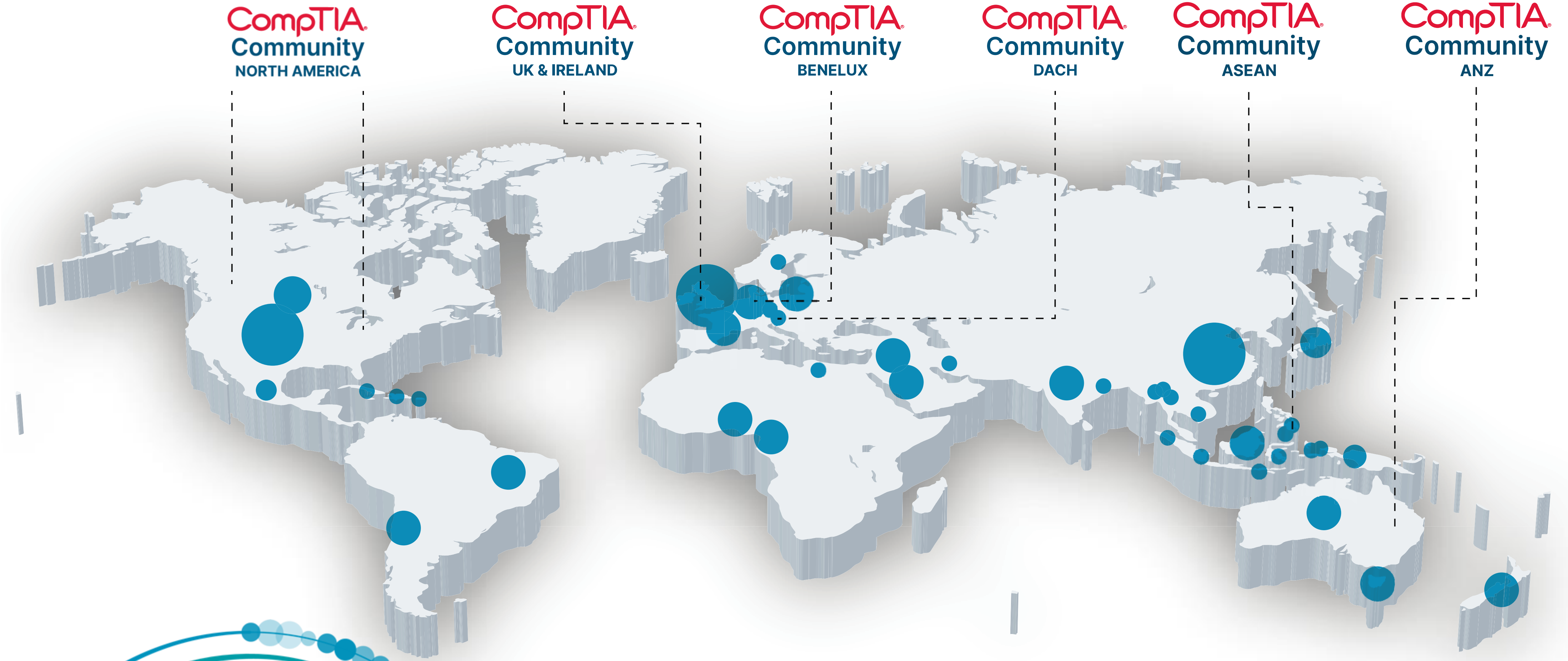
Manager, ANZ and ASEAN Regional Groups

WE ARE THE

CompTIA Community

Regional Groups

CompTIA Community


CompTIA Community NORTH AMERICA
CompTIA Community UK & IRELAND
CompTIA Community BENELUX
CompTIA Community DACH
CompTIA Community ASEAN
CompTIA Community ANZ

Regional Groups

CompTIA Community

CompTIA Community NORTH AMERICA	CompTIA Community UK & IRELAND	CompTIA Community BENELUX	CompTIA Community DACH	CompTIA Community ASEAN	CompTIA Community ANZ
Canada	United Kingdom	Belgium	Germany	Brunei Darussalam	Australia
United States	Ireland	Netherlands	Austria	Cambodia	New Zealand
		Luxembourg	Switzerland	Indonesia	
				Lao PDR	
				Malaysia	
				Myanmar	
				Philippines	
				Singapore	
				Thailand	
				Viet Nam	

WE ARE THE CompTIA Community

Our Member Regions Across The Globe

New groups representing additional regions are always being considered.
For current information on member groups, visit connect.comptia.org.

Interest Groups

CompTIA Community

CompTIA Community NORTH AMERICA	CompTIA Community UK & IRELAND	CompTIA Community BENELUX	CompTIA Community DACH	CompTIA Community ASEAN	CompTIA Community ANZ
Advancing Women in Tech Diversity, Equity & Inclusion Cybersecurity Managed Services	Advancing Women in Tech Diversity, Equity & Inclusion Cybersecurity Emerging Tech Managed Services	Advancing Women in Tech Diversity, Equity & Inclusion Cybersecurity Emerging Tech Managed Services	Cybersecurity Emerging Tech Managed Services	Cybersecurity Emerging Tech Managed Services	Cybersecurity Emerging Tech Managed Services

WE ARE THE CompTIA Community

Interest Groups Across The Globe

New groups representing additional regions are always being considered.
For current information on member groups, visit connect.comptia.org.

Record Setting Events in Every Region

CompTIA Community

ASEAN

ANZ Spotlight Awards

EMEA Member and Partner Conference

ChannelCon

Benelux

CompTIA Community Forum

DACH

YOUR MISSION TODAY

rstamell@comptia.org

#CompTIACommunity

MENTORSHIP?

Mentors need to be working for a CompTIA Community Member Company.

Mentees can be anyone in the community.

INTEREST GROUPS

Are you a Subject Matter Expert?

Do you want to lead regular community discussions?

Regional Groups

July

- ChannelCon (Atlanta)
- Interest Group Call: I got AntiVirus, I'm sorted, aren't I?

August

- CompTIA Cybersecurity Risk Management Workshop at CRN Pipeline,
- CompTIA Cybersecurity Risk Management Workshop at IT Nation.
- Risk Management Interest Group Call

September

- ANZ Regional Meetings in Auckland, Sydney and Adelaide

October

- CompTIA at SMBiT Professionals National Conference 2024. Oct 25-26

November

- ASEAN CompTIA Regional Meetings in Jakarta, Manila and Ho Chi Minh City

Adelaide Agenda

CompTIA Community

TIME	TOPIC
09:15 – 09:45 AM	**Welcome & Introduction** MJ Shoer, Chief Community Officer, CompTIA
09:45 – 10:00 AM	**Privacy Act Changes Impacting Your Business** David Norris, Managing Director, Nortec IT, Dean Calvert, Founder, Calvert Technologies
10:00 – 10:30 AM	**State of Cybersecurity.** David Norris, Managing Director, Nortec IT
10:30 – 11:00 AM	**MORNING TEA & NETWORKING BREAK**
11:00 – 11:30 AM	**Securing Active Directory:** KRBTGT Resets After Credential Theft. Samuel Freeman, Senior Investigator DFIR, CyberCX
11:30 AM – 12:30 PM	**Risk Management for your business. Part 1.** Wayne Selk, VP Cybersecurity Programs, CompTIA
12:30 – 12:35 PM	**QUICK BREAK**
12:35 – 1:00 PM	**State of the Channel, with ANZ Perspectives.** Maria Armstrong, Manager of Academy APAC, Pax8
1:00 – 2:00 PM	**LUNCH & NETWORKING**

Adelaide Agenda

CompTIA Community

TIME	TOPIC
2:00 – 2:20 PM	**A Comedy Spot** after lunch with Rob Farley.
2:25 – 3:05 PM	**Why Your Customers Need Cybersecurity Insurance.** Andrew Bremner, SherpaTech
3:05 – 3:10 PM	**QUICK BREAK**
3:10 – 4:00 PM	**Risk Management for your business. Part 2.** Wayne Selk, VP, Cybersecurity Programs, CompTIA
4:00 – 4:05 PM	**QUICK BREAK**
4:00 – 4:30 PM	**Fireside Chat** MJ Shoer & Wayne Selk – CompTIA
4:30 – 5:00 PM	**NETWORKING DRINKS & CANAPES**

Adelaide Agenda

TIME	TOPIC
09:15 – 09:45 AM	**Welcome & Introduction** MJ Shoer, Chief Community Officer, CompTIA
09:45 – 10:00 AM	**Privacy Act Changes Impacting Your Business** David Norris, Managing Director, Nortec IT, Dean Calvert, Founder, Calvert Technologies
10:00 – 10:30 AM	**State of Cybersecurity** David Norris, Managing Director, Nortec IT
10:30 – 11:00 AM	**MORNING TEA & NETWORKING BREAK**
11:00 – 11:30 AM	**Securing Active Directory:** KRBTGT Resets After Credential Theft. Samuel Freeman, Senior Investigator DFIR, CyberCX
11:30 AM – 12:30 PM	**Risk Management for your business. Part 1.** Wayne Selk, VP Cybersecurity Programs, CompTIA
12:30 – 12:35 PM	**QUICK BREAK**
12:35 – 1:00 PM	**State of the Channel, with ANZ Perspectives.** Maria Armstrong, Manager of Academy APAC, Pax8
1:00 – 2:00 PM	**LUNCH & NETWORKING**

WE ARE THE

CompTIA®

Community

PRIVACY ACT CHANGES IMPACTING YOUR BUSINESS

David Norris, MD, Nortech IT

Dean Calvert, CEO, Calvert Technologies/Blackbird IT

Privacy Act Changes

Recommended Changes

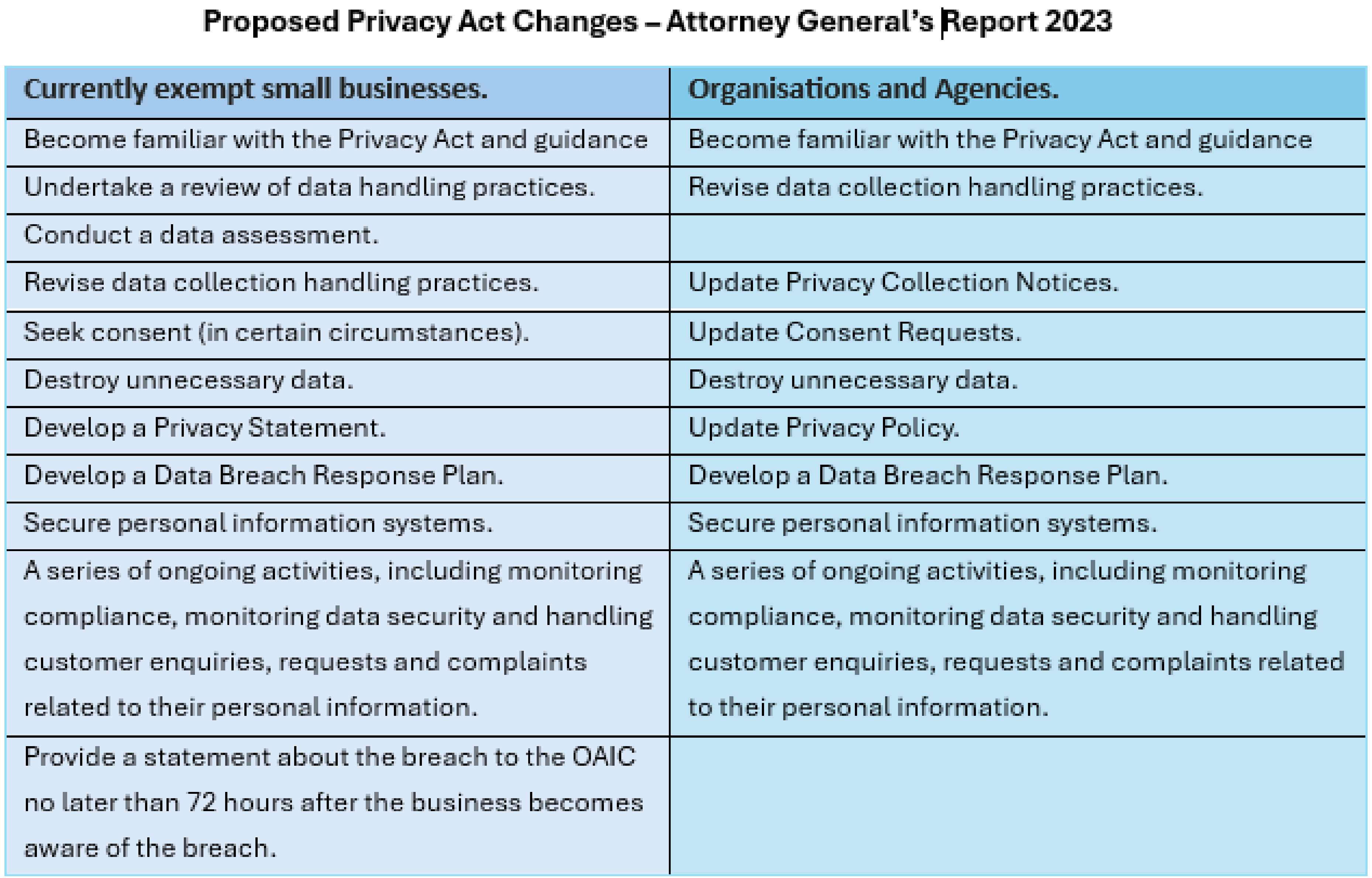
The Attorney-General’s Department has been hard at work, and their review of the Privacy Act 1988 has yielded a whopping **116 proposals**.

Alignment with the EU’s GDPR:

- The proposed reforms aim to align Australia’s privacy laws more closely with the European Union’s **General Data Protection Regulation (GDPR)**.
- What does this mean? Expect stricter requirements for handling personal data, enhanced individual rights, and a greater emphasis on transparency.

Benefits:

- Protecting and supporting people in the event of an emergency.
- Improving individuals' confidence in collecting, using, and disclosing personal information.
- Reduction in inquiries and complaints about personal information.
- Reduced costs of data breaches.
- Reduction in fraud involving identity crime due to fewer data breaches



Proposed Privacy Act Changes – Attorney General's Report 2023

Currently exempt small businesses.	Organisations and Agencies.
Become familiar with the Privacy Act and guidance	Become familiar with the Privacy Act and guidance
Undertake a review of data handling practices.	Revise data collection handling practices.
Conduct a data assessment.	
Revise data collection handling practices.	Update Privacy Collection Notices.
Seek consent (in certain circumstances).	Update Consent Requests.
Destroy unnecessary data.	Destroy unnecessary data.
Develop a Privacy Statement.	Update Privacy Policy.
Develop a Data Breach Response Plan.	Develop a Data Breach Response Plan.
Secure personal information systems.	Secure personal information systems.
A series of ongoing activities, including monitoring compliance, monitoring data security and handling customer enquiries, requests and complaints related to their personal information.	A series of ongoing activities, including monitoring compliance, monitoring data security and handling customer enquiries, requests and complaints related to their personal information.
Provide a statement about the breach to the OAIC no later than 72 hours after the business becomes aware of the breach.	

Opportunities

Tech Support Teams/ Managed Service Providers:

- Companies will need help navigating the privacy requirements, so they will turn to their technology support teams for guidance.
- As an industry, we need to understand what’s coming and start having conversations with our clients. Expect questions like, “Hey, how do we ensure compliance with the new rules?”
- Discuss the changes, decode the legalese, and offer practical advice.
- Compliance comes with a price tag. There will be costs associated with meeting the new requirements.

Privacy Act Changes

The reforms proposed by the Attorney-General's Department were built around five key themes:

1. bringing the Privacy Act into the digital age,
2. uplifting privacy protections,
3. increasing clarity and simplicity for entities and individuals,
4. improving transparency and control, and
5. strengthening enforcement.

The reforms featured in the Bill have largely focussed on the last theme of strengthening enforcement. Changes in other areas will have to wait for a later date.

Watered Down

My Opinion—The government will fail to align Australian privacy legislation with international benchmarks and enhance individual data protections within the digital economy.

Giving the Office of the Australian Information Commissioner (OAIC) more power to enforce rules.

Introducing new levels of fines for breaking privacy laws.

A special privacy code is required for children’s online activities.

Making companies more transparent about how they use automated decision-making.

Creating a new law that lets people sue for serious privacy invasions.

Making ‘doxxing’ (sharing someone’s private information online to harm them) a specific crime."

What they Left Out

The introduction of a new general obligation to ensure all handling of personal information is ‘fair and reasonable’ – this was one of the marquee reform proposal.

An expansion of the definition of ‘personal information’ to cover online identifiers and other information that can be used to target individuals even without revealing their underlying legal identity;

New individual rights, such as rights to ask for information to be deleted and for online search engine results to be de-indexed;

The removal or narrowing of current exemptions for small businesses (of which there are approximately 2.5 million currently in Australia) and for employers dealing with employee records

Changes to rules around use of personal information for direct marketing and targeted advertising, including stronger opt-out rights;

rights for individuals to take direct action in court in response to breaches of the Privacy Act (something that would have further increased the prospects of seeing a more litigious privacy landscape in future).

Adelaide Agenda

TIME	TOPIC
09:15 – 09:45 AM	**Welcome & Introduction** MJ Shoer, Chief Community Officer, CompTIA
09:45 – 10:00 AM	**Privacy Act Changes Impacting Your Business** David Norris, Managing Director, Nortec IT, Dean Calvert, Founder, Calvert Technologies
10:00 – 10:30 AM	**State of Cybersecurity.** David Norris, Managing Director, Nortec IT
10:30 – 11:00 AM	**MORNING TEA & NETWORKING BREAK**
11:00 – 11:30 AM	**Securing Active Directory:** KRBTGT Resets After Credential Theft. Samuel Freeman, Senior Investigator DFIR, CyberCX
11:30 AM – 12:30 PM	**Risk Management for your business. Part 1.** Wayne Selk, VP Cybersecurity Programs, CompTIA
12:30 – 12:35 PM	**QUICK BREAK**
12:35 – 1:00 PM	**State of the Channel, with ANZ Perspectives.** Maria Armstrong, Manager of Academy APAC, Pax8
1:00 – 2:00 PM	**LUNCH & NETWORKING**

WE ARE THE

CompTIA®

Community

STATE OF CYBERSECURITY

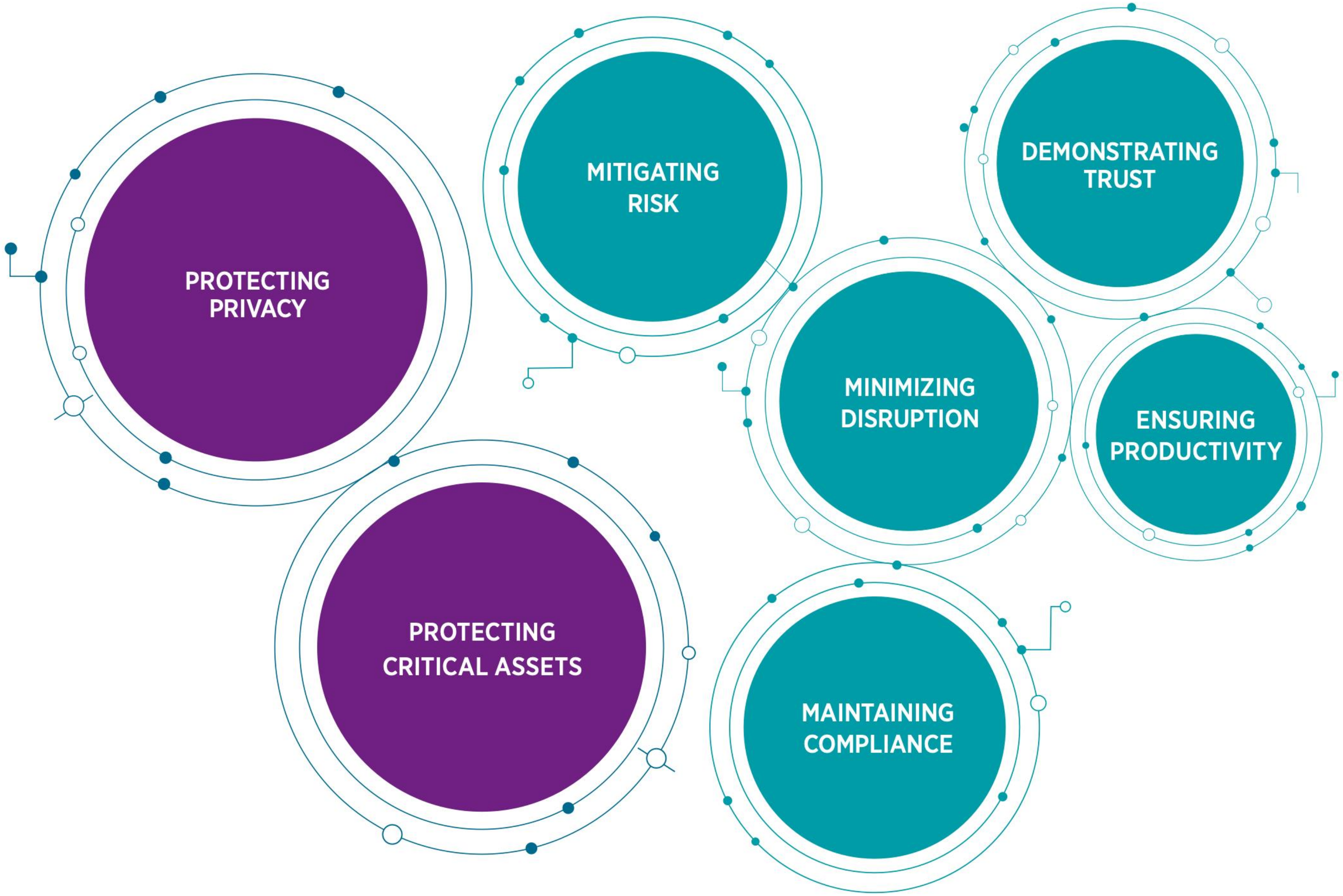
David Norris, MD, Nortech IT

CompTIA

State of Cybersecurity 2024
ANZ

Objectives for Cybersecurity

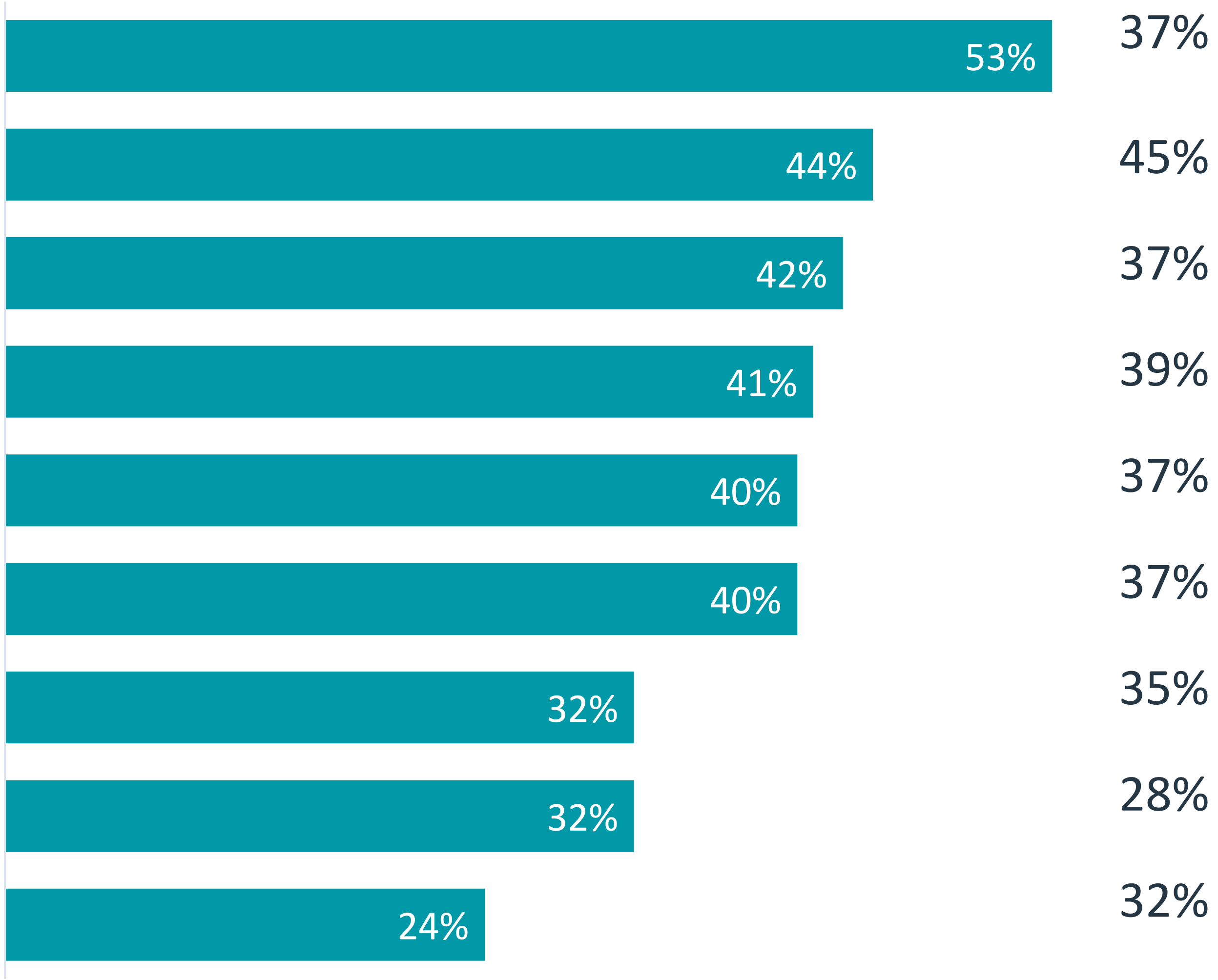
Aggregated priority of objectives across ASEAN, ANZ, Benelux, DACH, North America and UK/Ireland



CompTIA

Source: CompTIA 2024 State of Cybersecurity | n=1156 technical and business professionals

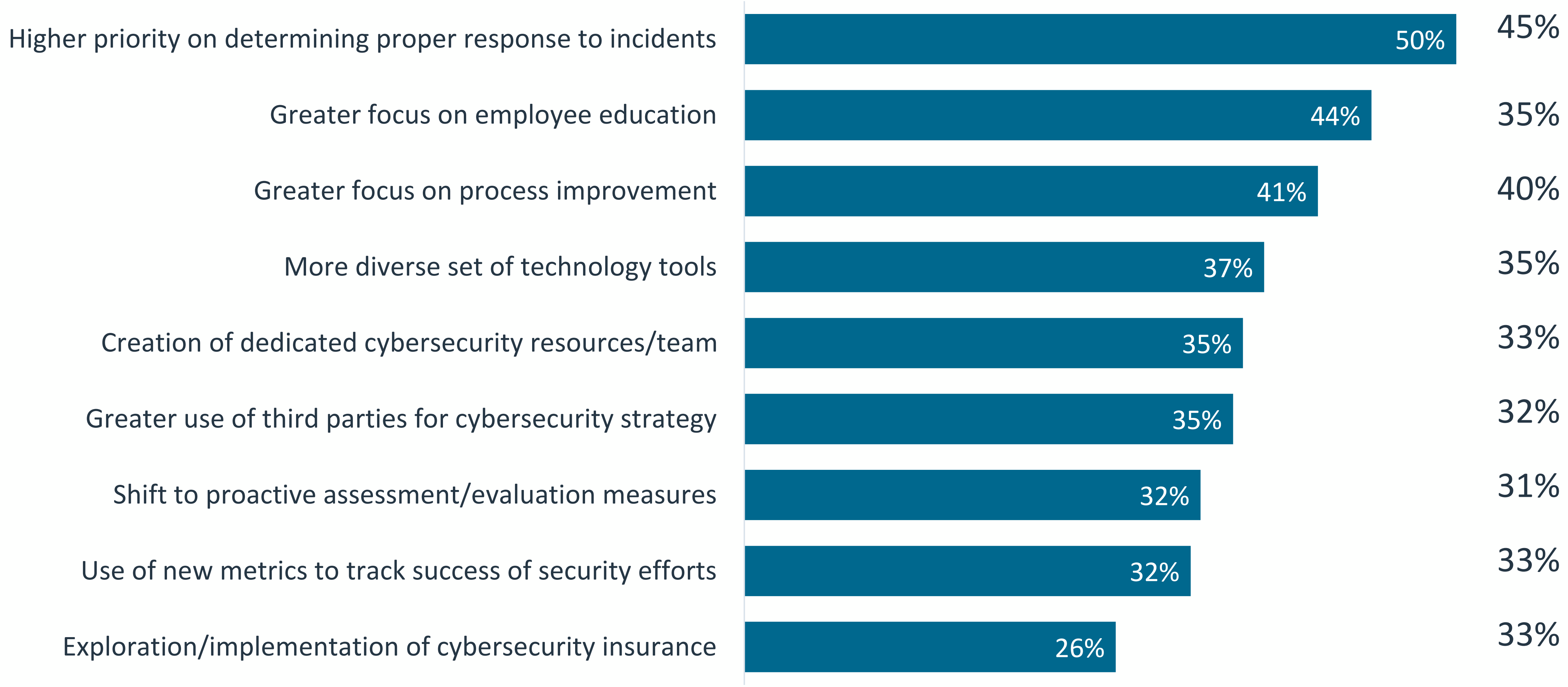
Many Issues Drive Cybersecurity Concerns



CompTIA.

Source: CompTIA 2024 State of Cybersecurity | n=133 ANZ technical and business professionals

Cybersecurity Changes In the Past Year

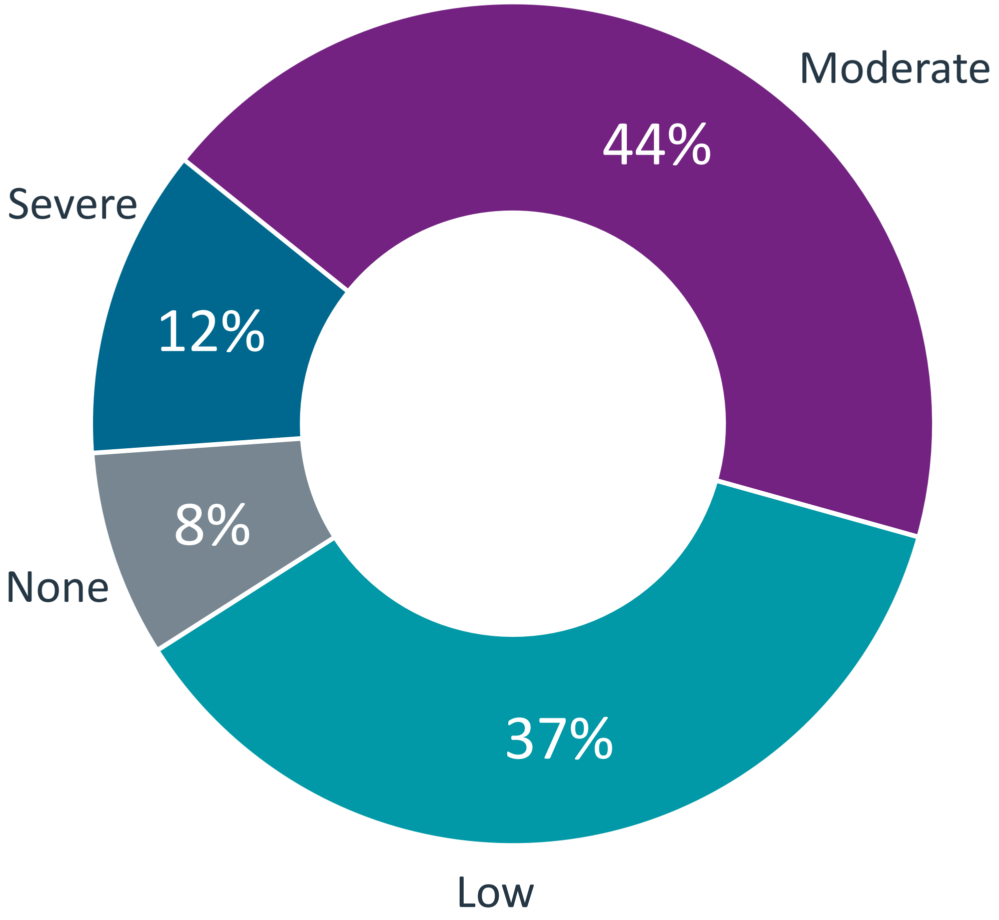


CompTIA

Source: CompTIA 2024 State of Cybersecurity | n=133 ANZ technical and business professionals

Mitigating Cybersecurity Incidents in the Past Year

Estimated Impact of Incidents



Common Mitigation Steps

1 Technical staff working overtime

2 Technical staff diverted from routine

3 Purchase new software

4 Business staff prevented from workflow

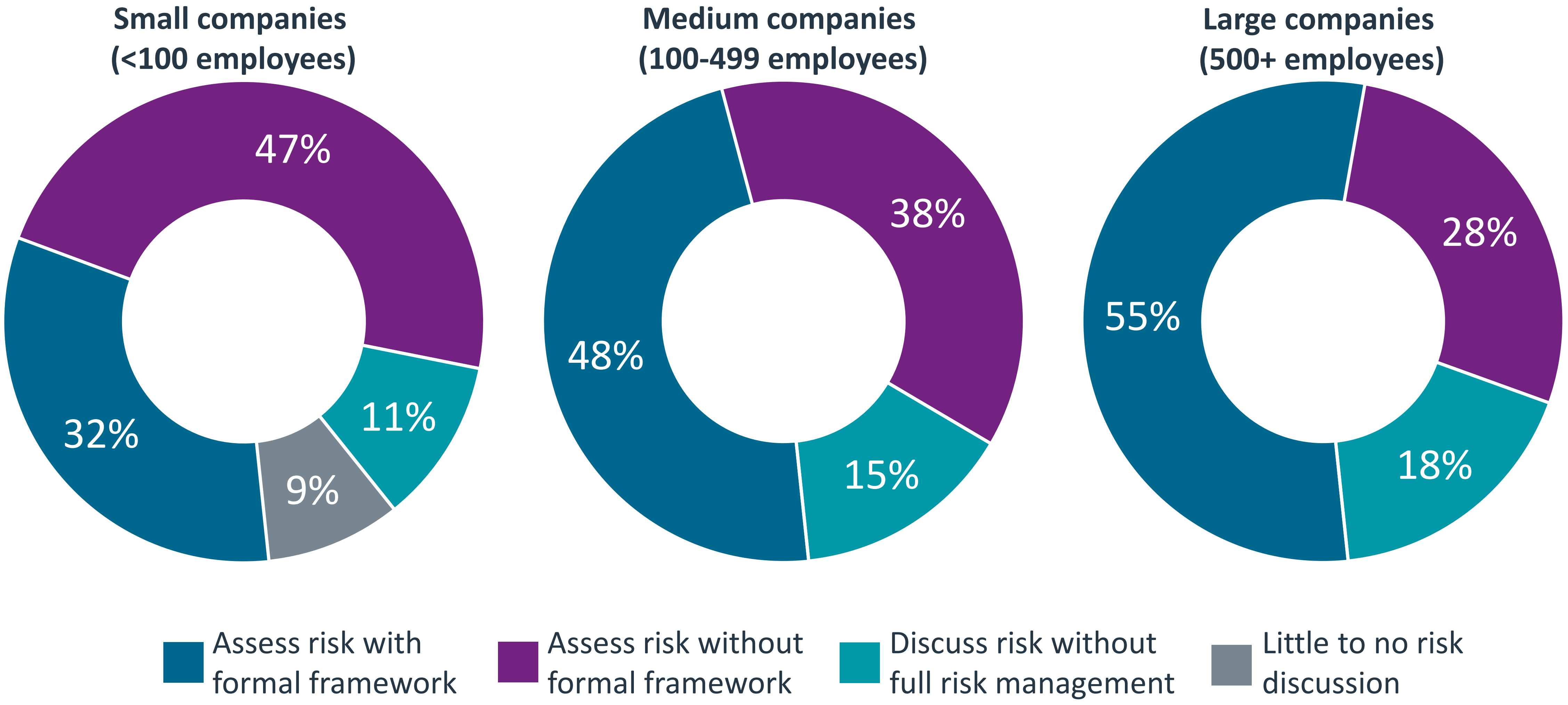
5 Purchase new hardware

6 Outside specialist brought in

7 External communication plan

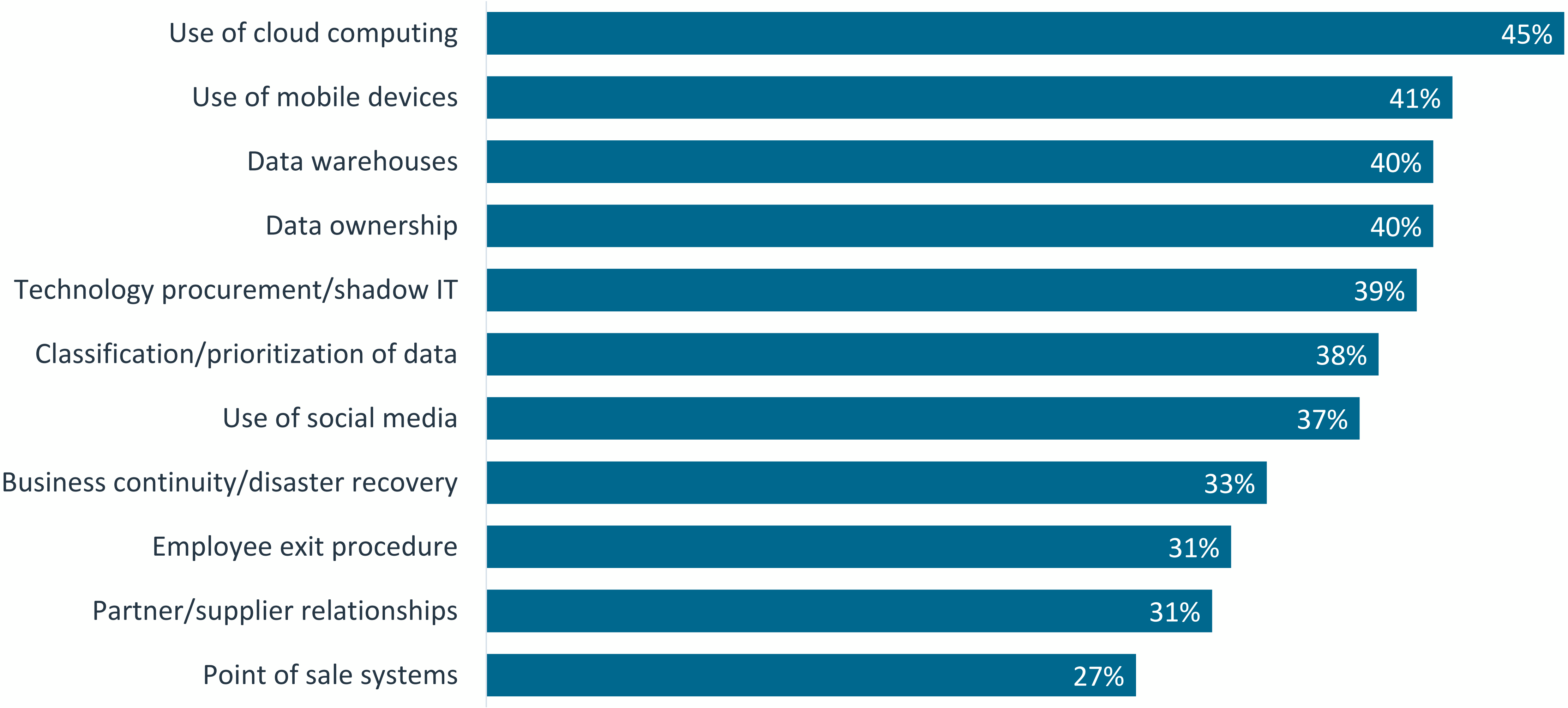
Source: CompTIA 2024 State of Cybersecurity | n=133 ANZ technical and business professionals

Organizational Approaches to Risk Management



Source: CompTIA 2024 State of Cybersecurity | n=133 ANZ technical and business professionals

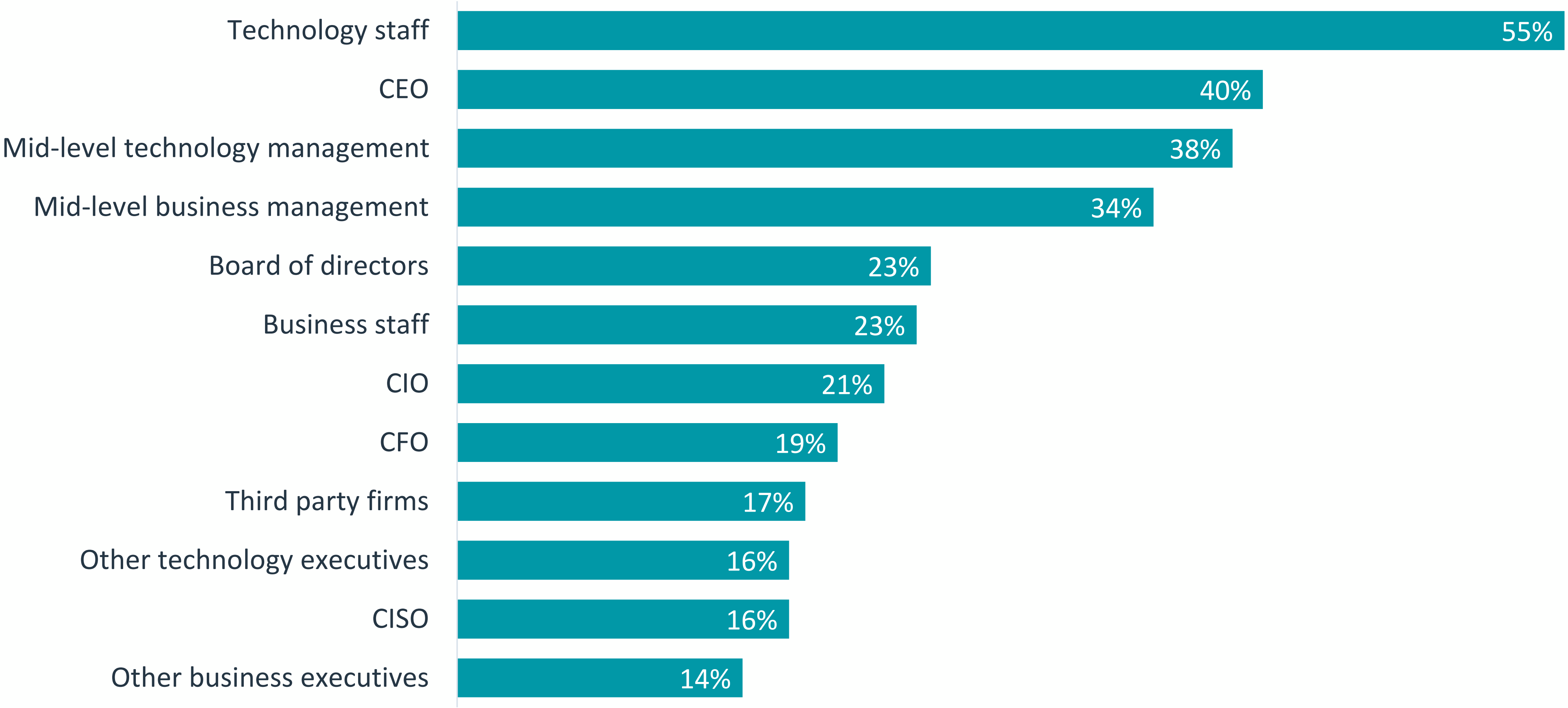
Topics Included in Risk Analysis



CompTIA

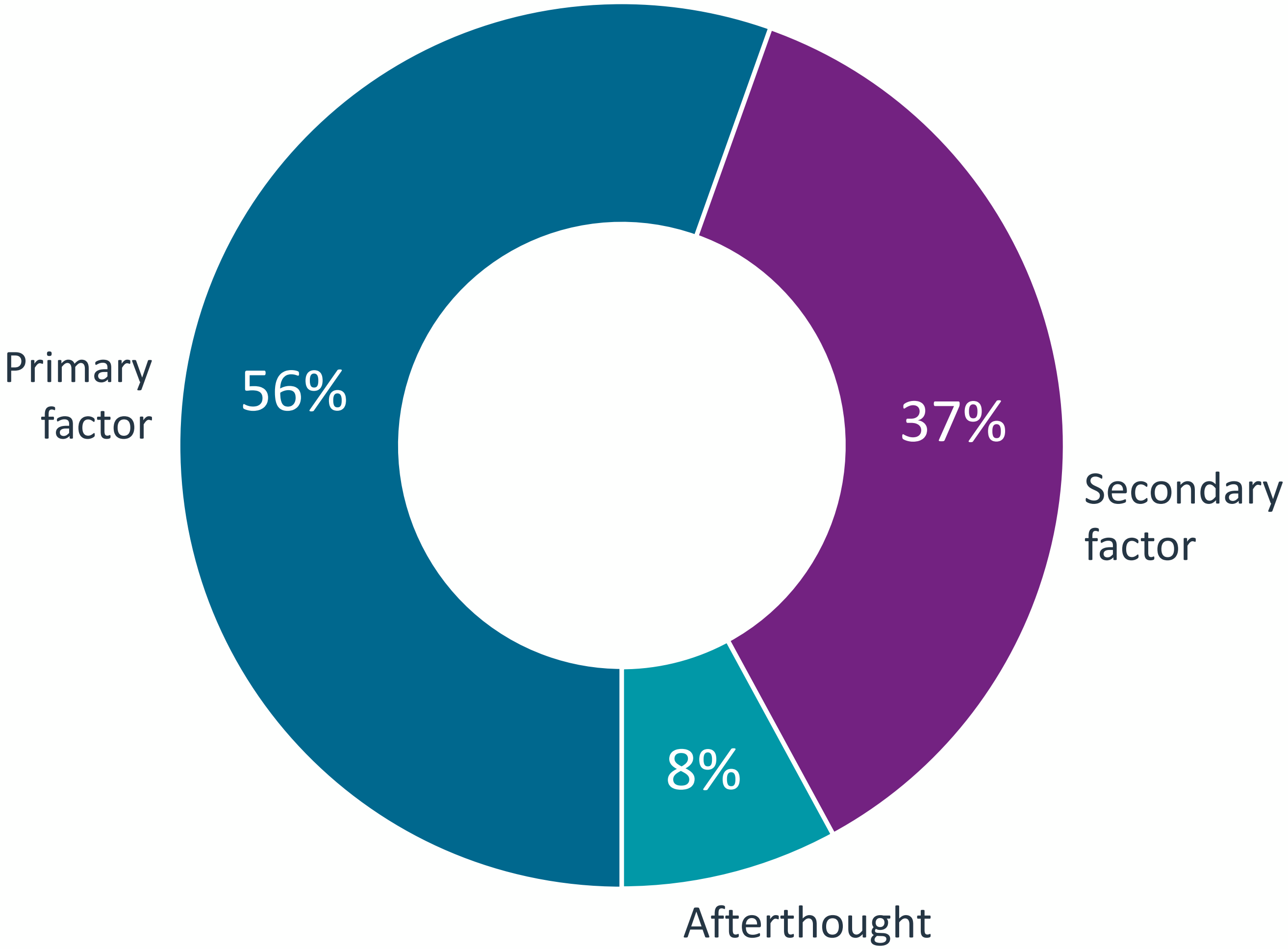
Source: CompTIA 2024 State of Cybersecurity | n=128 ANZ technical and business professionals

People Involved in Risk Management Discussions



Source: CompTIA 2024 State of Cybersecurity | n=128 ANZ technical and business professionals

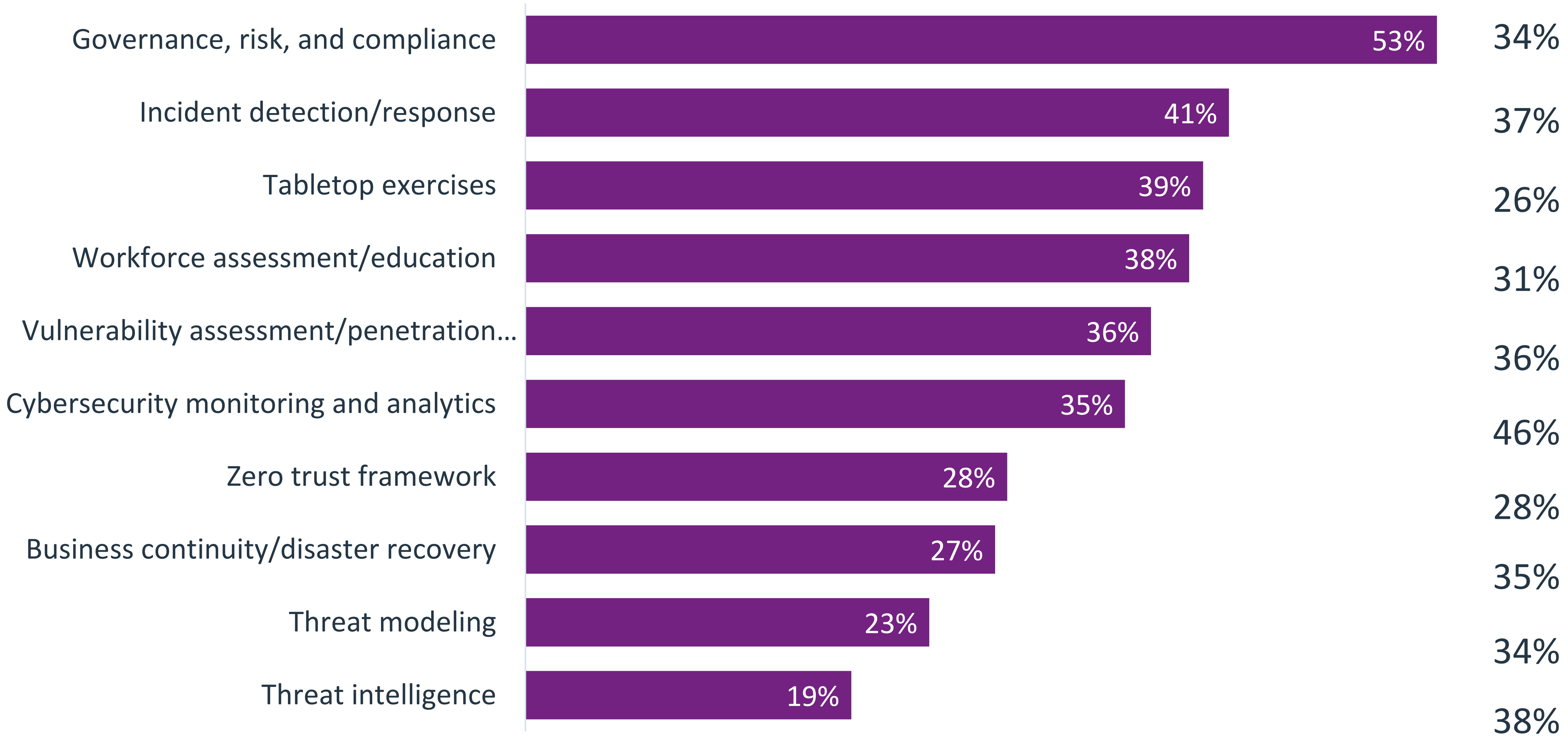
The Role of Cybersecurity in Assessing Technology



The interconnected nature of technology initiatives driving digital transformation creates an even greater demand for cybersecurity planning in early assessment

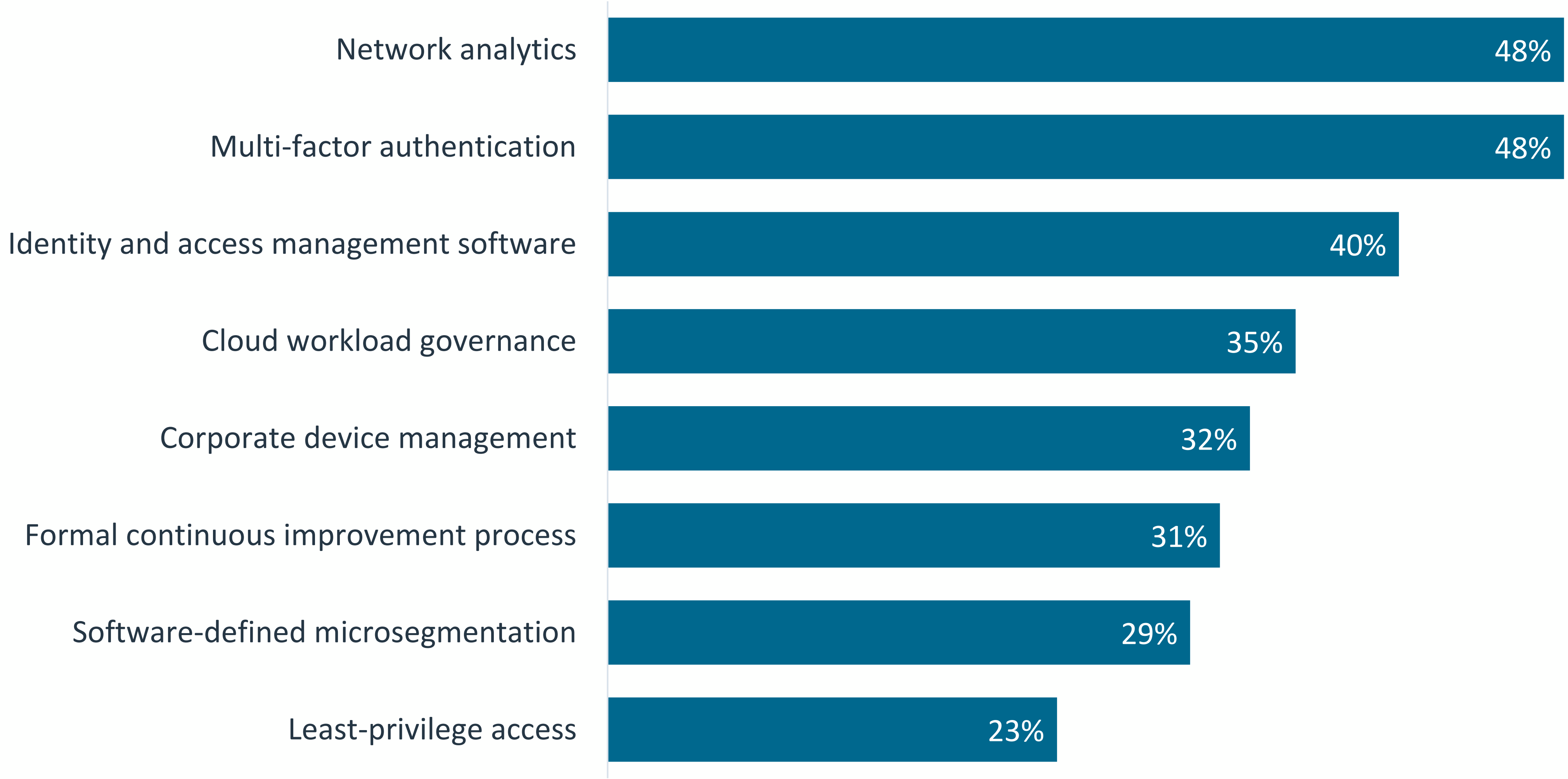
Source: CompTIA 2024 State of Cybersecurity | n=133 ANZ technical and business professionals

Elements of Organizational Cybersecurity Strategy



Source: CompTIA 2024 State of Cybersecurity | n=133 ANZ technical and business professionals

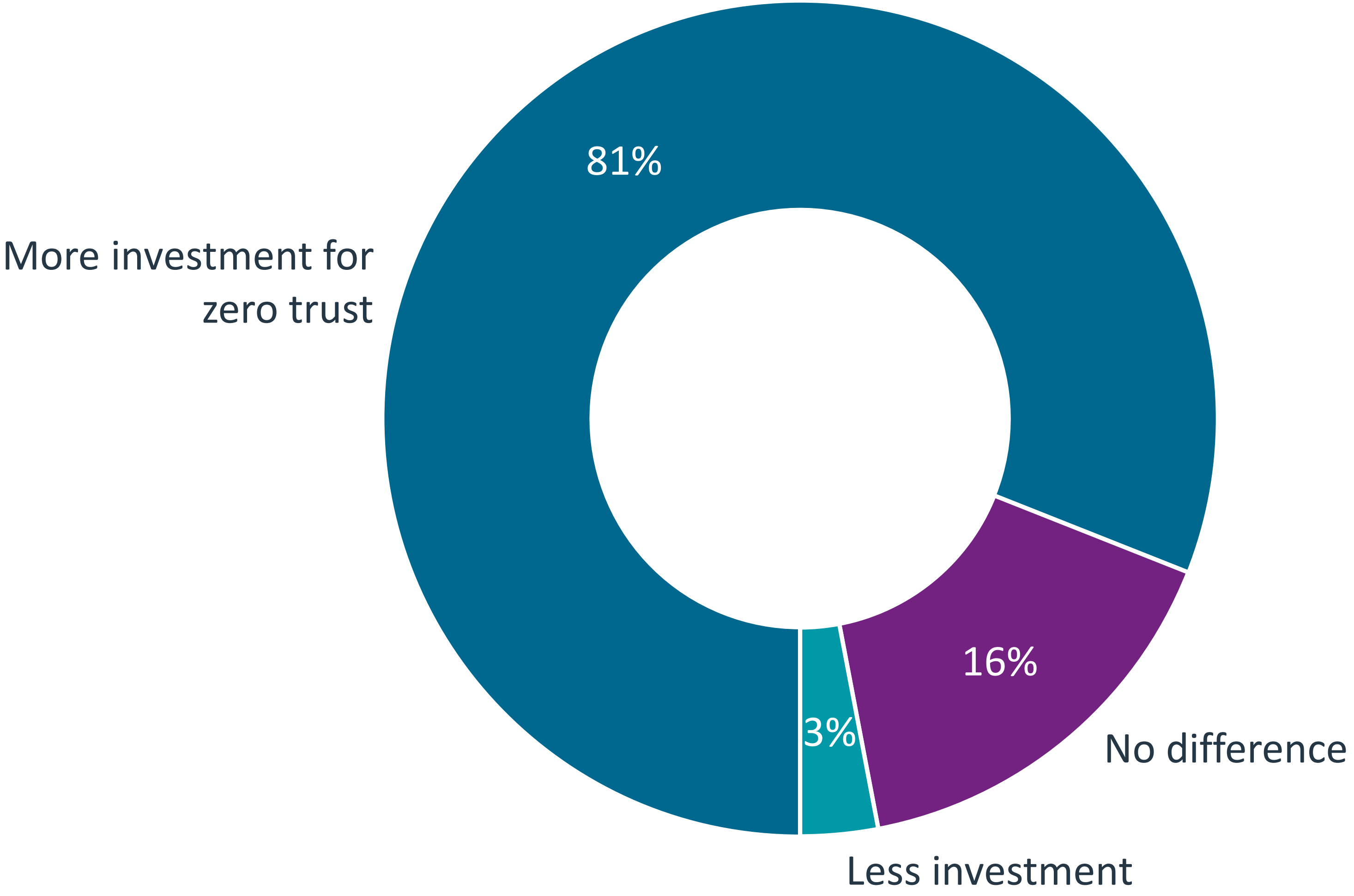
Practices Included in Cybersecurity Strategy



CompTIA

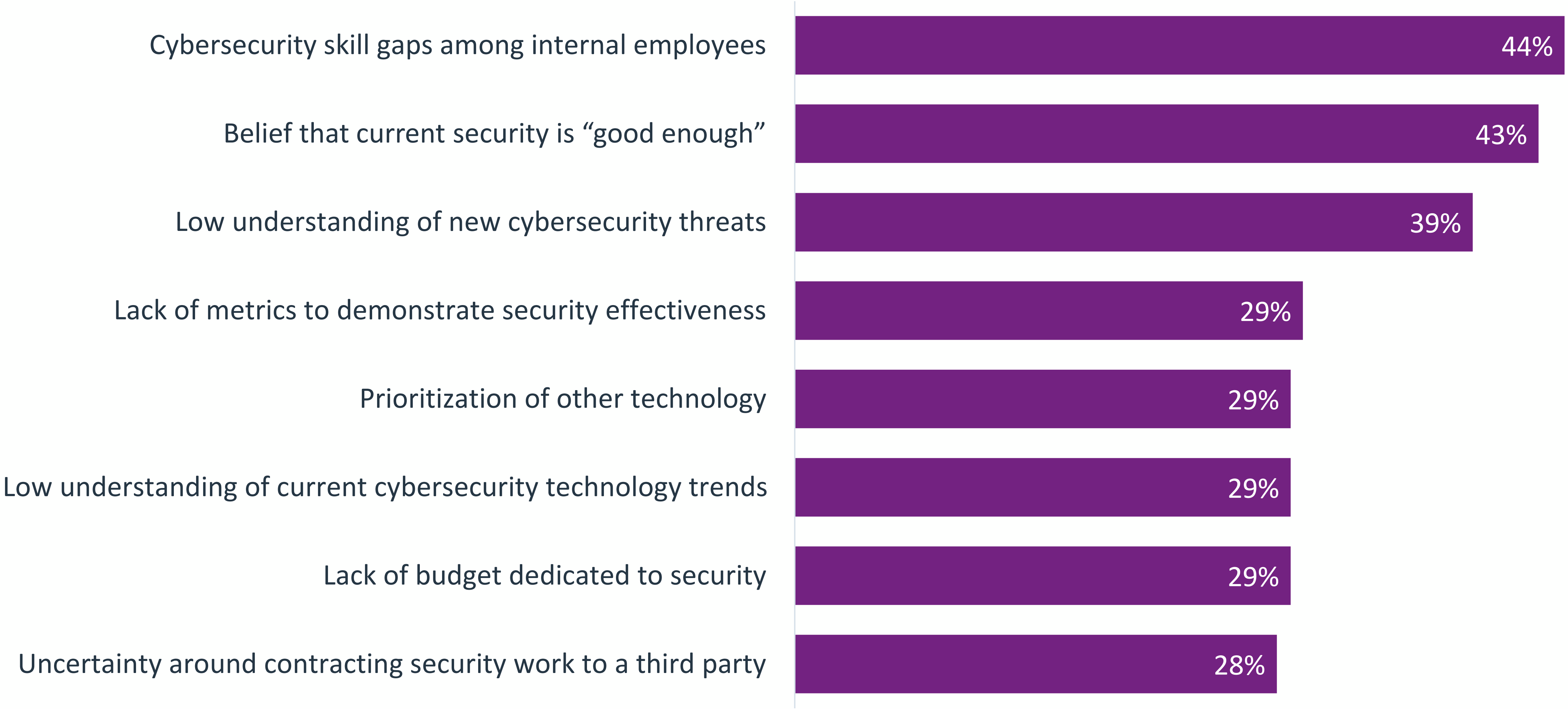
Source: CompTIA 2024 State of Cybersecurity | n=133 ANZ technical and business professionals

Zero Trust Framework Investment vs Prior Cybersecurity Investment



Source: CompTIA 2024 State of Cybersecurity | n=37 ANZ technical and business professionals using a zero trust framework

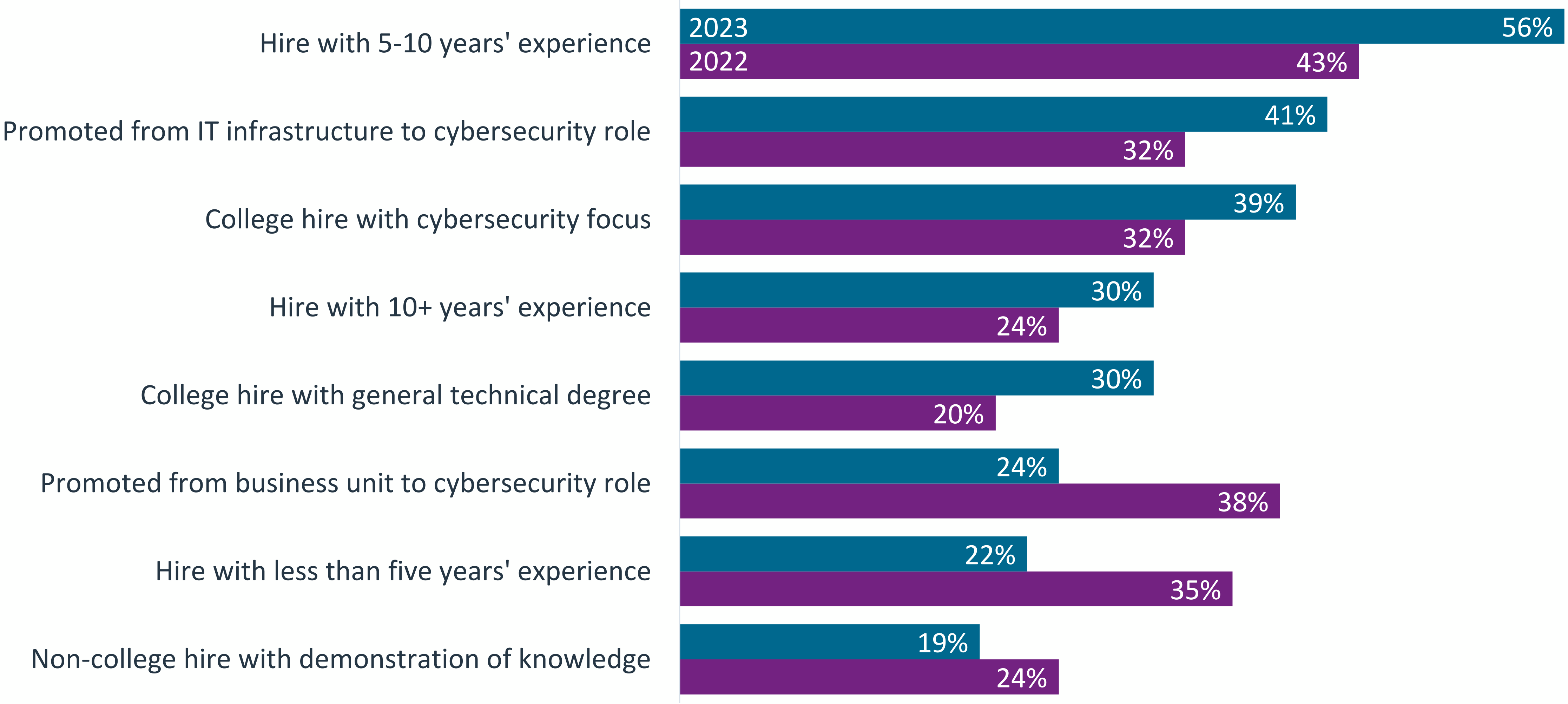
Challenges to Cybersecurity Initiatives



CompTIA

Source: CompTIA 2024 State of Cybersecurity | n=133 ANZ technical and business professionals

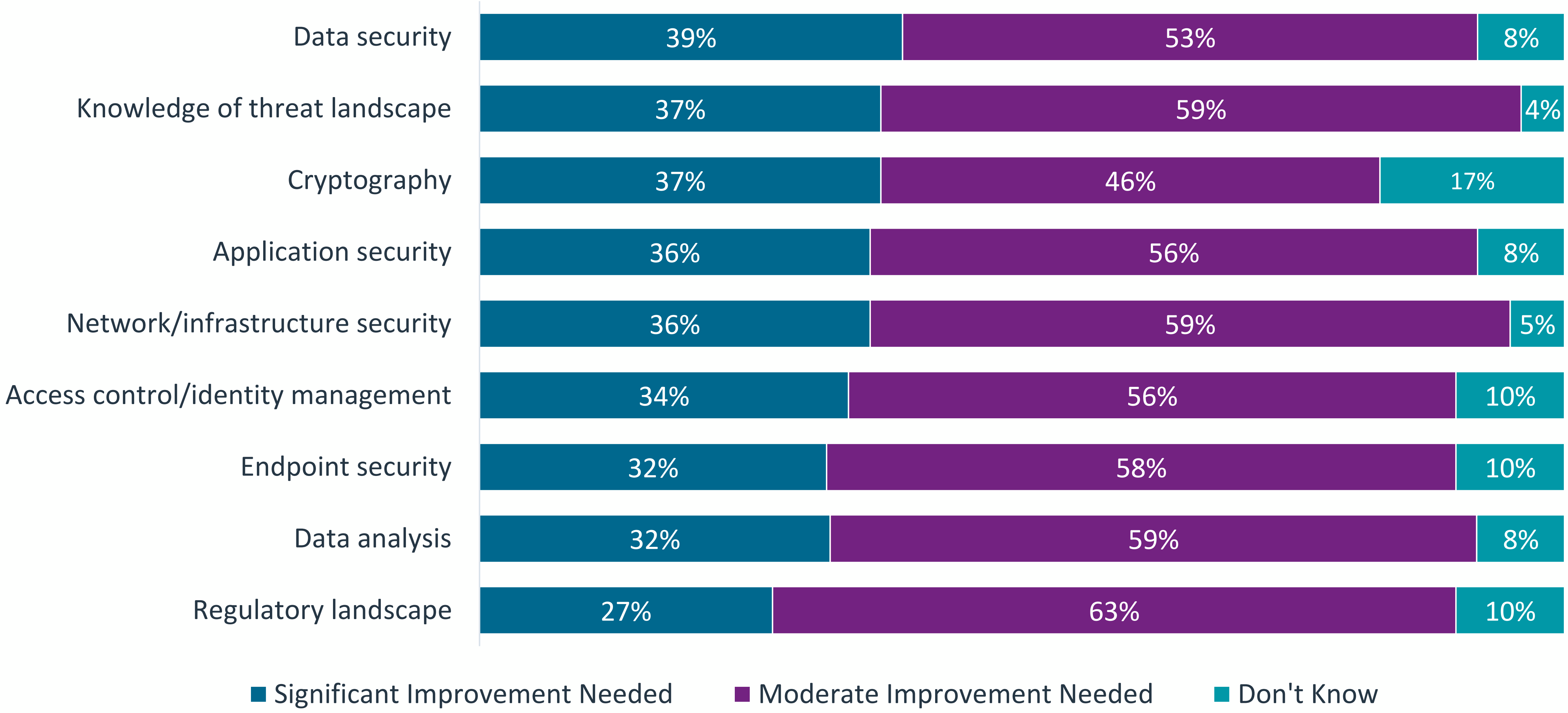
Pathways for Dedicated Cybersecurity Personnel



CompTIA

Source: CompTIA 2024 State of Cybersecurity | n=54 ANZ technical and business professionals with hiring plans
CompTIA 2022 State of Cybersecurity | n=74 ANZ technical and business professionals with hiring plans

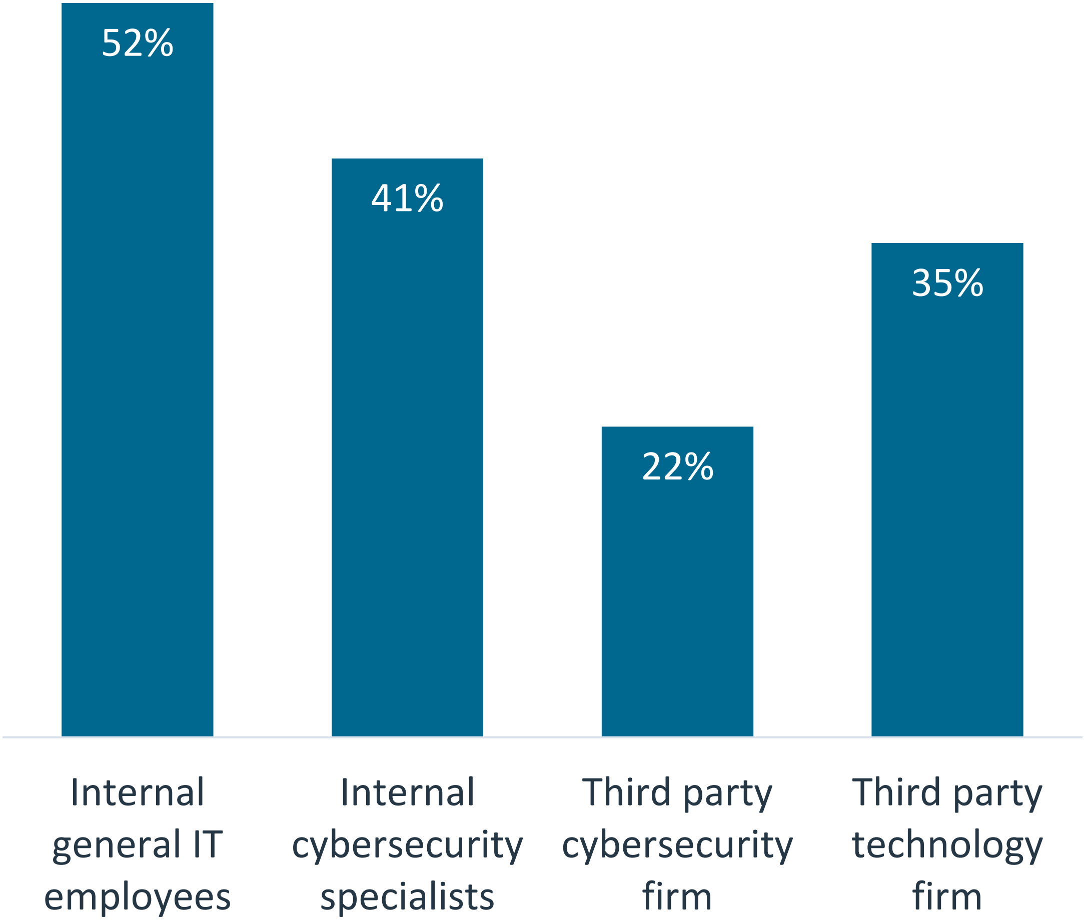
Areas of Improvement for Cybersecurity Personnel



CompTIA

Source: CompTIA 2024 State of Cybersecurity | n=133 ANZ technical and business professionals

Groups Involved in Cybersecurity Initiatives



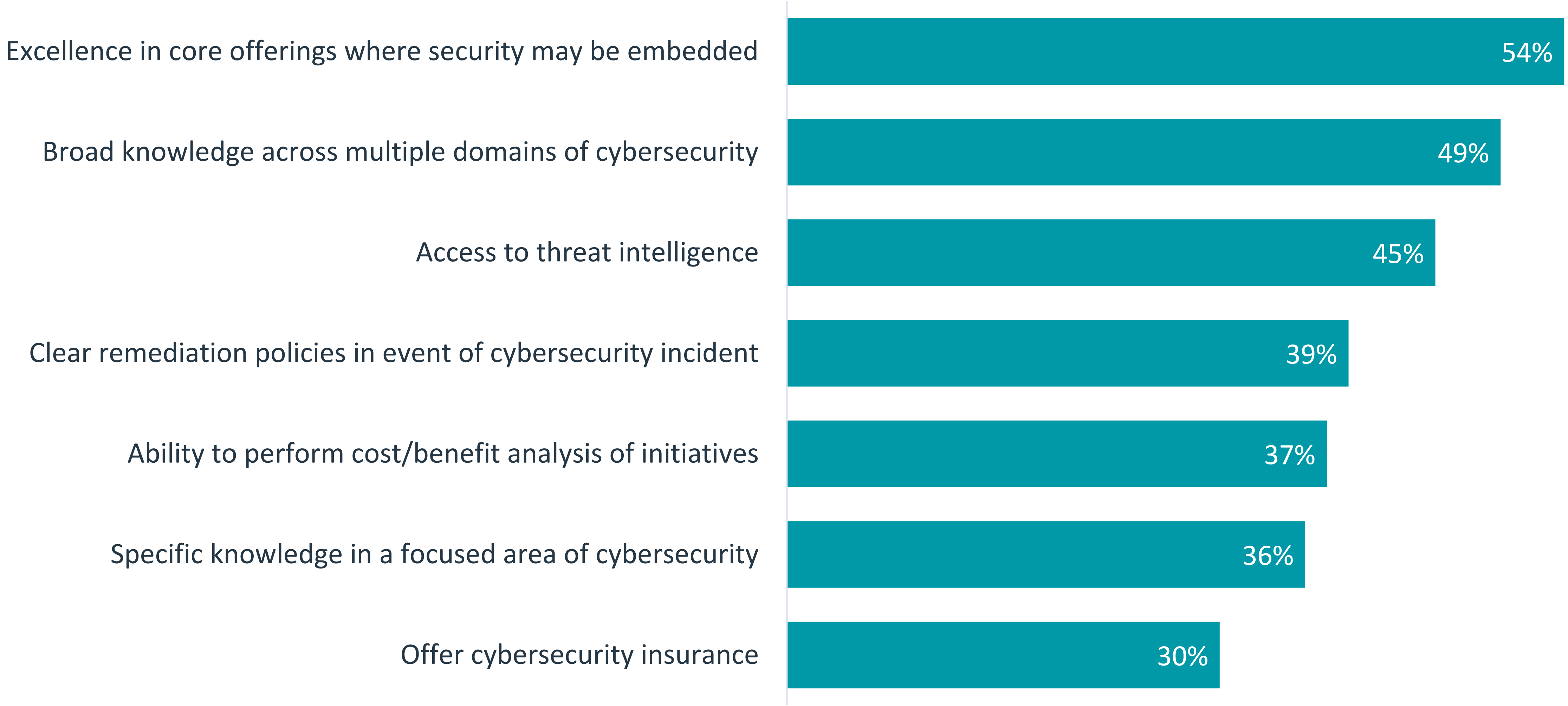
Types of third parties used

1. Managed service provider with many core IT offerings
2. Managed service provider exclusively focused on cybersecurity
3. General security firm offering both cybersecurity and physical security
4. Cloud providers with security embedded into offerings
5. Firm providing technical business services

CompTIA.

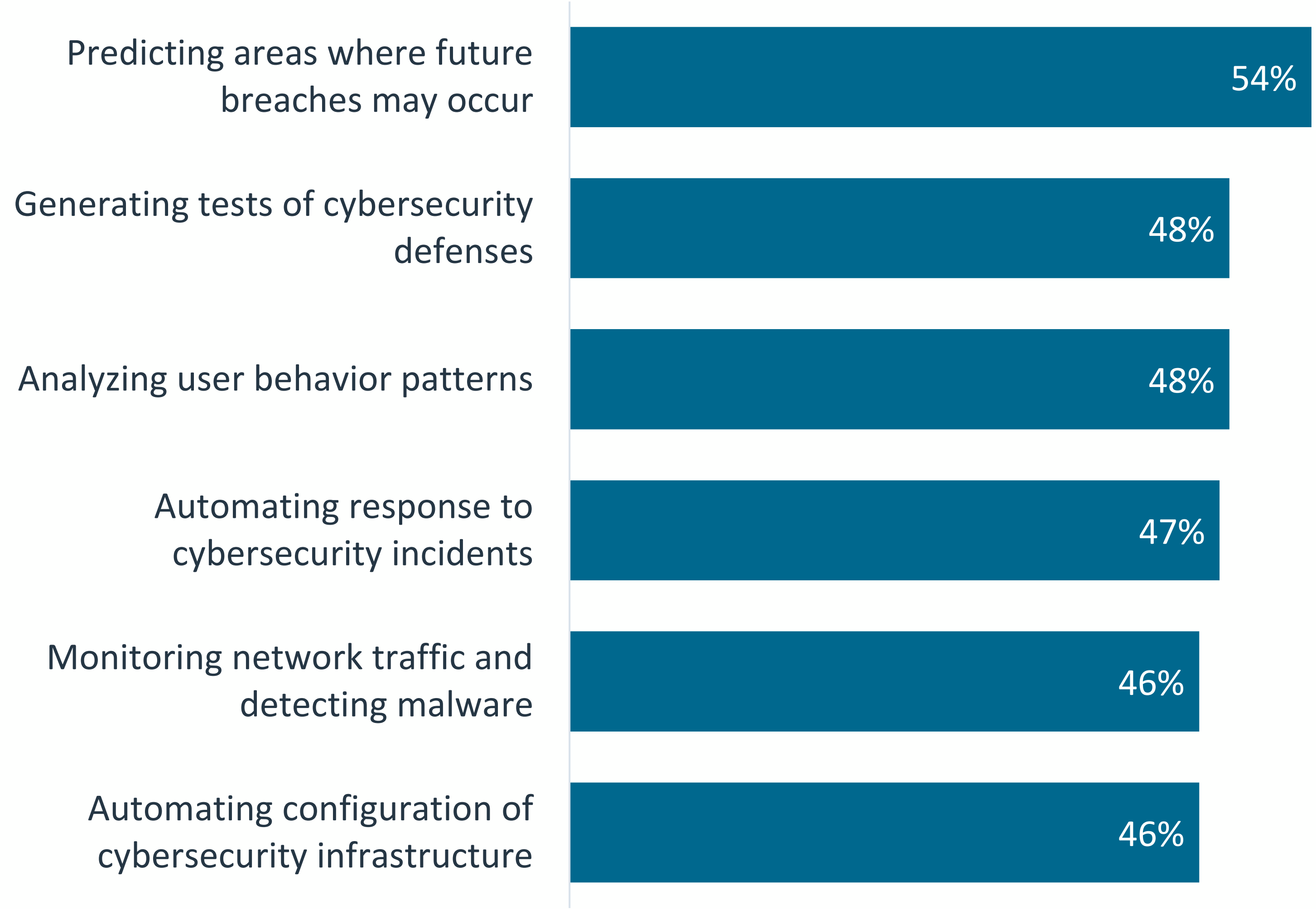
Source: CompTIA 2024 State of Cybersecurity | n=133 ANZ technical and business professionals
n=67 ANZ technical and business professionals using third parties for cybersecurity strategy

Criteria Used in Selecting Third-Party Firms



Source: CompTIA 2024 State of Cybersecurity | n=67 ANZ technical and business professionals using third parties for cybersecurity strategy

Potential Uses of AI in Cybersecurity

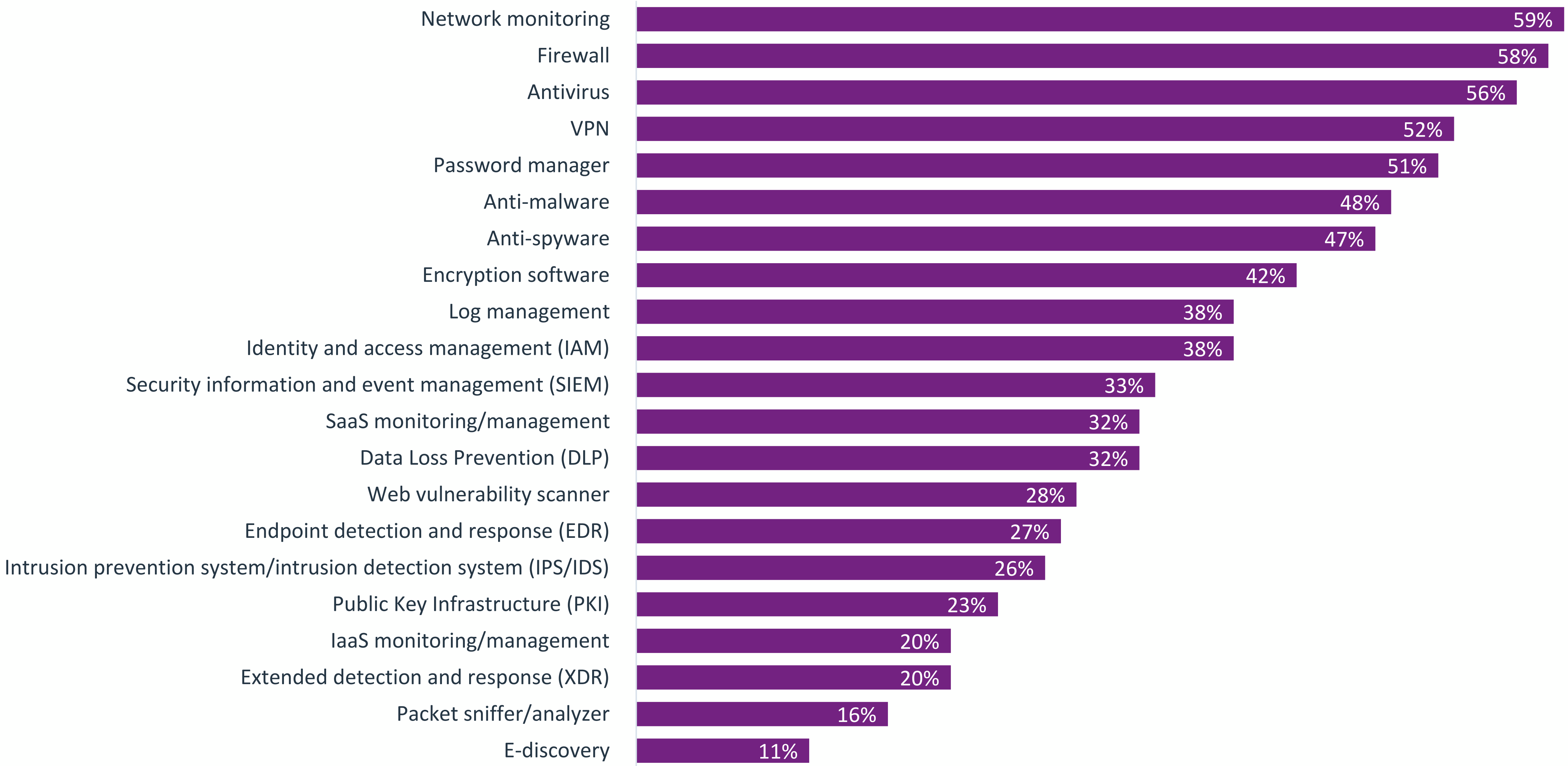


43% of organizations surveyed view generative AI as a step forward in existing AI/ML practices. Another 43% say that generative AI is driving first-time exploration of AI adoption.

CompTIA

Source: CompTIA 2024 State of Cybersecurity | n=133 ANZ technical and business professionals

Cybersecurity Products in Use



Source: CompTIA 2024 State of Cybersecurity | n=133 ANZ technical and business professionals

Methodology

CompTIA's *State of Cybersecurity* study provides insights around key career cybersecurity trends.

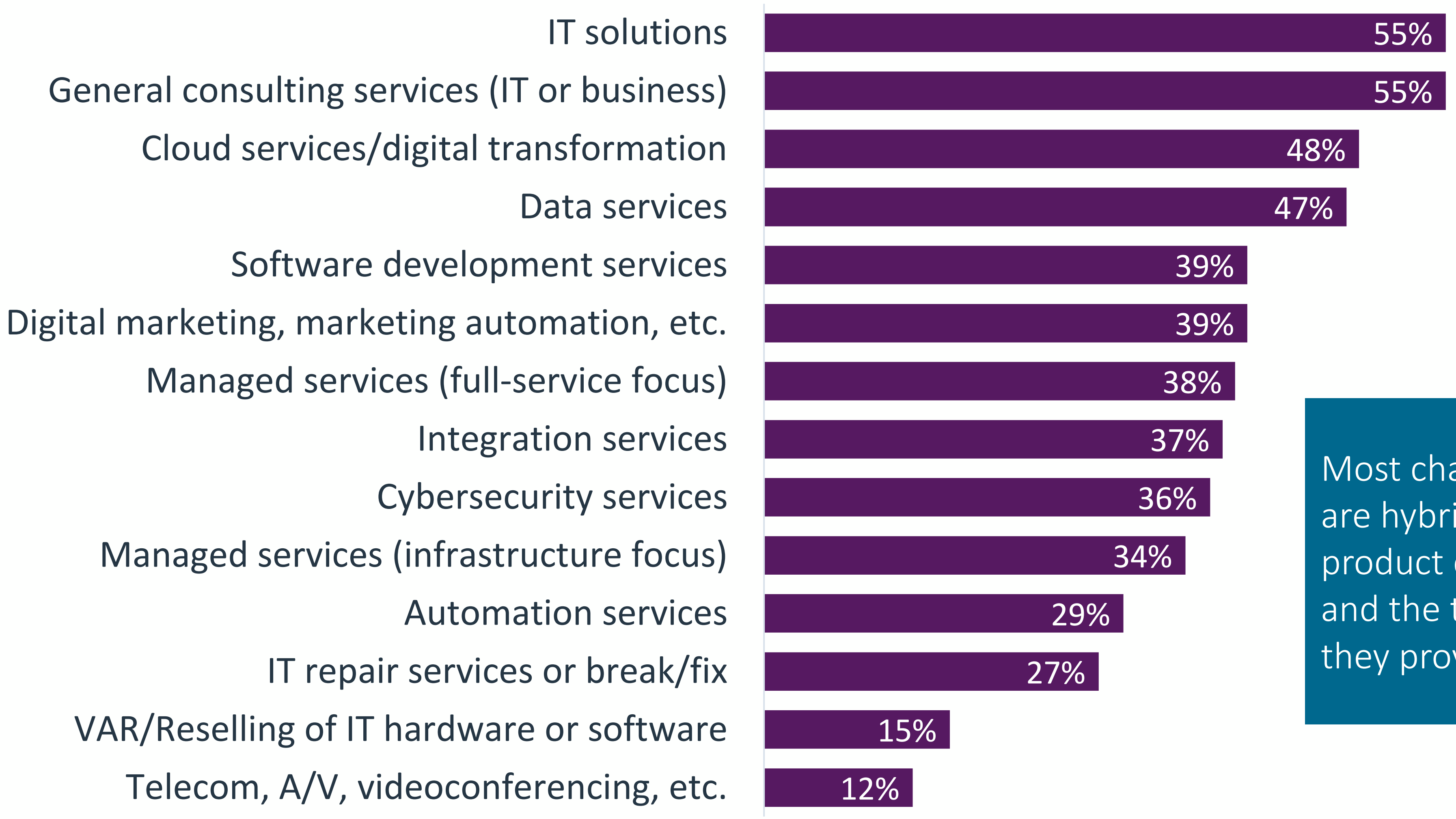
The quantitative study within the ANZ region consisted of an online survey fielded to IT professionals during July 2023. A total of 133 respondents participated in the survey, yielding an overall margin of sampling error at 95% confidence of +/- 8.7 percentage points. Sampling error is larger for subgroups of the data.

As with any survey, sampling error is only one source of possible error. While non-sampling error cannot be accurately calculated, precautionary steps were taken in all phases of the survey design, collection and processing of the data to minimize its influence.

CompTIA is responsible for all content and analysis. Any questions regarding the study should be directed to CompTIA Research and Market Intelligence staff at research@comptia.org.

CompTIA is a member of the market research industry's Insights Association and adheres to its internationally respected Code of Standards and Ethics.

Company Lines of Business Offered

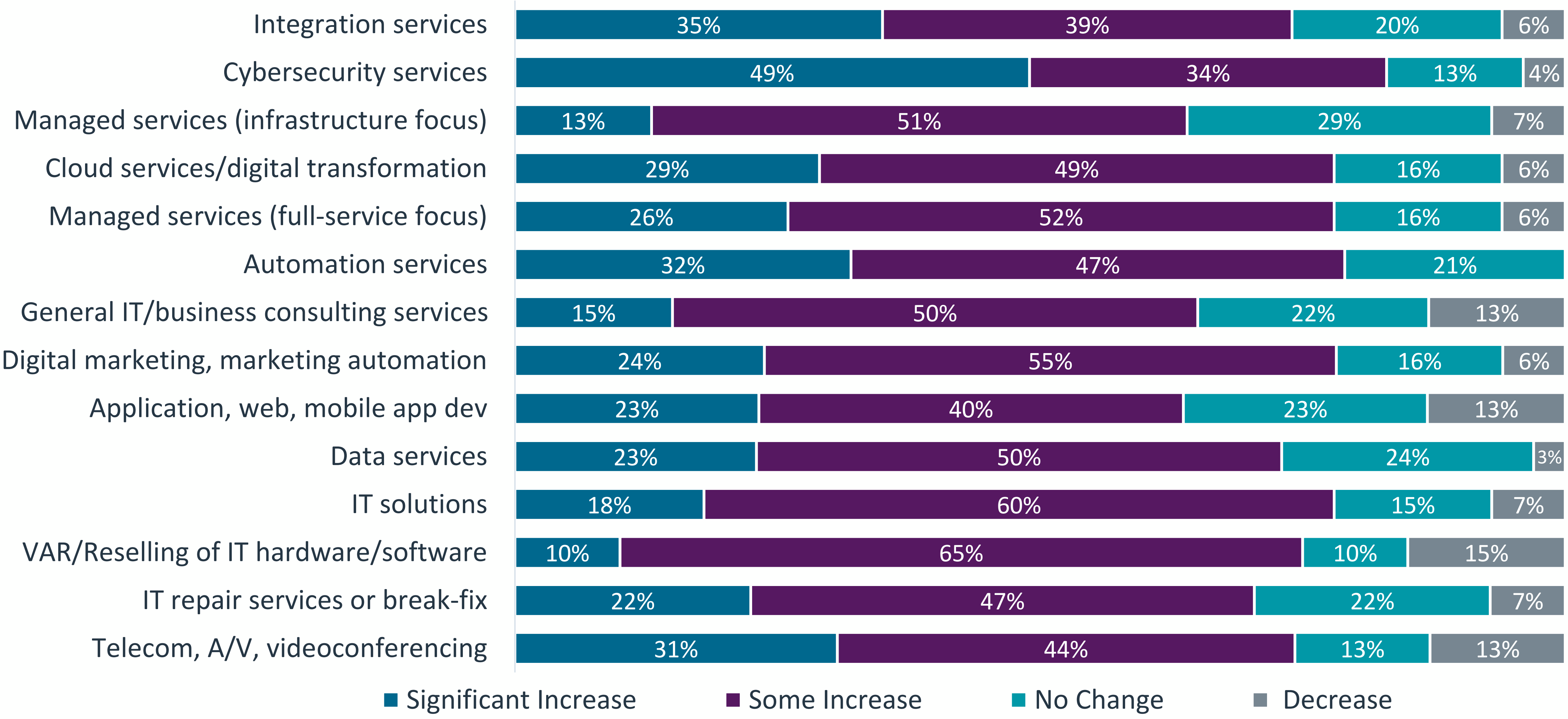


Most channel firms today are hybrid in terms of their product category offerings and the types of services they provide to customers.

CompTIA

Source: CompTIA 2024 State of the Channel survey | n=132 ANZ respondents

Revenue Growth Expected Over Next Two Years



CompTIA

Source: CompTIA 2024 State of the Channel survey | n=132 ANZ respondents

Adelaide Agenda

CompTIA Community

TIME	TOPIC
09:15 – 09:45 AM	**Welcome & Introduction** MJ Shoer, Chief Community Officer, CompTIA
09:45 – 10:00 AM	**Privacy Act Changes Impacting Your Business** David Norris, Managing Director, Nortec IT, Dean Calvert, Founder, Calvert Technologies
10:00 – 10:30 AM	**State of Cybersecurity.** David Norris, Managing Director, Nortec IT
10:30 – 11:00 AM	**MORNING TEA & NETWORKING BREAK**
11:00 – 11:30 AM	**Securing Active Directory:** KRBTGT Resets After Credential Theft. Samuel Freeman, Senior Investigator DFIR, CyberCX
11:30 AM – 12:30 PM	**Risk Management for your business. Part 1.** Wayne Selk, VP Cybersecurity Programs, CompTIA
12:30 – 12:35 PM	**QUICK BREAK**
12:35 – 1:00 PM	**State of the Channel, with ANZ Perspectives.** Maria Armstrong, Manager of Academy APAC, Pax8
1:00 – 2:00 PM	**LUNCH & NETWORKING**

WE ARE THE CompTIA® Community

10:30 – 11:00 AM

MORNING TEA & NETWORKING

Adelaide Agenda

CompTIA Community

TIME	TOPIC
09:15 – 09:45 AM	**Welcome & Introduction** MJ Shoer, Chief Community Officer, CompTIA
09:45 – 10:00 AM	**Privacy Act Changes Impacting Your Business** David Norris, Managing Director, Nortec IT, Dean Calvert, Founder, Calvert Technologies
10:00 – 10:30 AM	**State of Cybersecurity.** David Norris, Managing Director, Nortec IT
10:30 – 11:00 AM	**MORNING TEA & NETWORKING BREAK**
11:00 – 11:30 AM	**Securing Active Directory:** KRBTGT Resets After Credential Theft. Samuel Freeman, Senior Investigator DFIR, CyberCX
11:30 AM – 12:30 PM	**Risk Management for your business. Part 1.** Wayne Selk, VP Cybersecurity Programs, CompTIA
12:30 – 12:35 PM	**QUICK BREAK**
12:35 – 1:00 PM	**State of the Channel, with ANZ Perspectives.** Maria Armstrong, Manager of Academy APAC, Pax8
1:00 – 2:00 PM	**LUNCH & NETWORKING**

WE ARE THE CompTIA® Community

11:00 - 11:15 AM

SECURING ACTIVE DIRECTORY AFTER CREDENTIAL THEFT

Samuel Freeman, Senior Investigator DFIR, CyberCX

SECURING Active DIRECTORY

KRBTGT RESETS AFTER CREDENTIAL THEFT

- 10 Years in Systems Administration and Cyber at the RAAF
- 6 Months in Digital Forensics at the AFP
- 3 Years in Full Time DFIR at CyberCX
- GCFA, GNFA, GDAT, GCFR

Intro to Active Directory

Credential Theft Attacks

Eradication

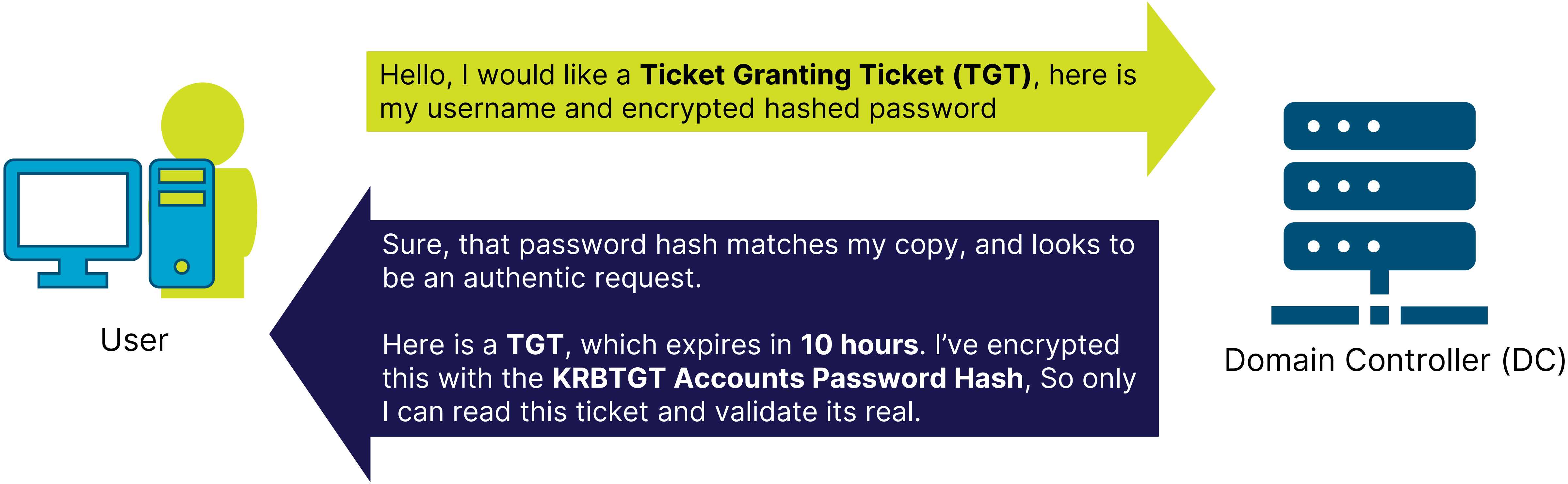
Lessons Learned in the Field

Intro to Active Directory

Active Directory is a service developed by Microsoft for Windows Server, which provides authentication for Users and Computers

Key Terms:

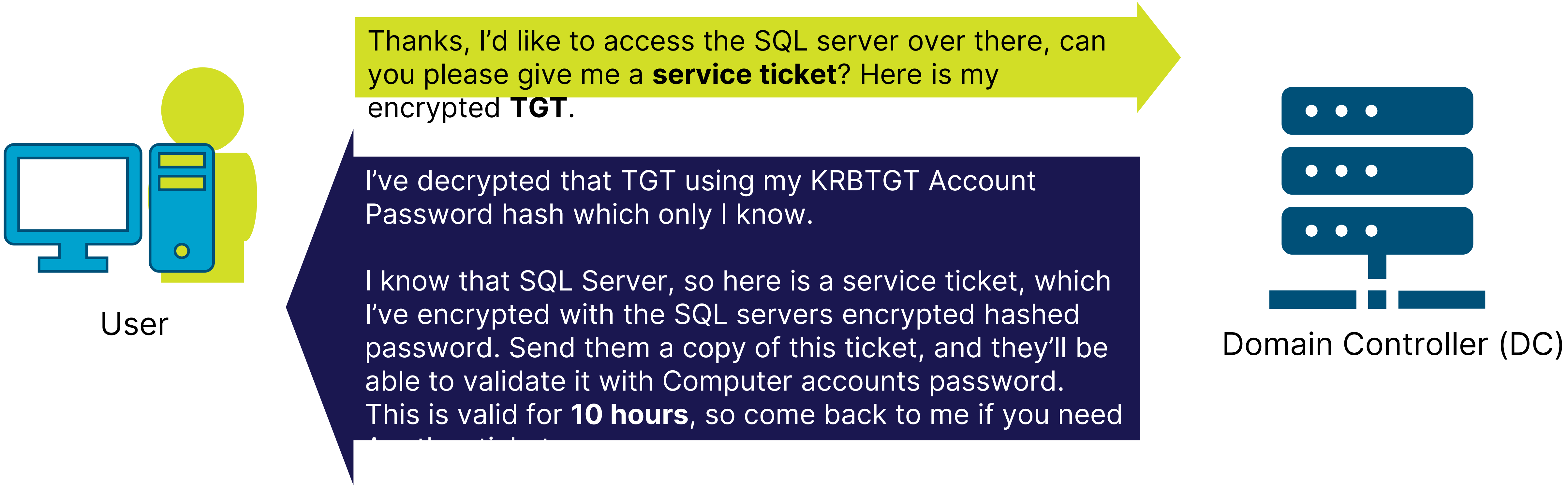
- Domain – A logical structure of containers and objects including users and computers
- Domain Controller (DC) - A server running the Active Directory Domain Services role
- Replication – The process for replicating the changes made to objects between domain controllers
- Kerberos – The protocol used by Active Directory to authenticate users and computers
- Trust – A trusted link between one or more domains in Active Directory
- KRBTGT – Kerberos Ticket Granting Ticket
- Password Hash – A transformed or encrypted transformation of a password



Hello, I would like a **Ticket Granting Ticket (TGT)**, here is my username and encrypted hashed password

Sure, that password hash matches my copy, and looks to be an authentic request.

Here is a **TGT**, which expires in **10 hours**. I’ve encrypted this with the **KRBTGT Accounts Password Hash**, So only I can read this ticket and validate its real.



Thanks, I'd like to access the SQL server over there, can you please give me a **service ticket**? Here is my encrypted **TGT**.

I've decrypted that TGT using my KRBTGT Account Password hash which only I know.

I know that SQL Server, so here is a service ticket, which I've encrypted with the SQL servers encrypted hashed password. Send them a copy of this ticket, and they'll be able to validate it with Computer accounts password. This is valid for **10 hours**, so come back to me if you need

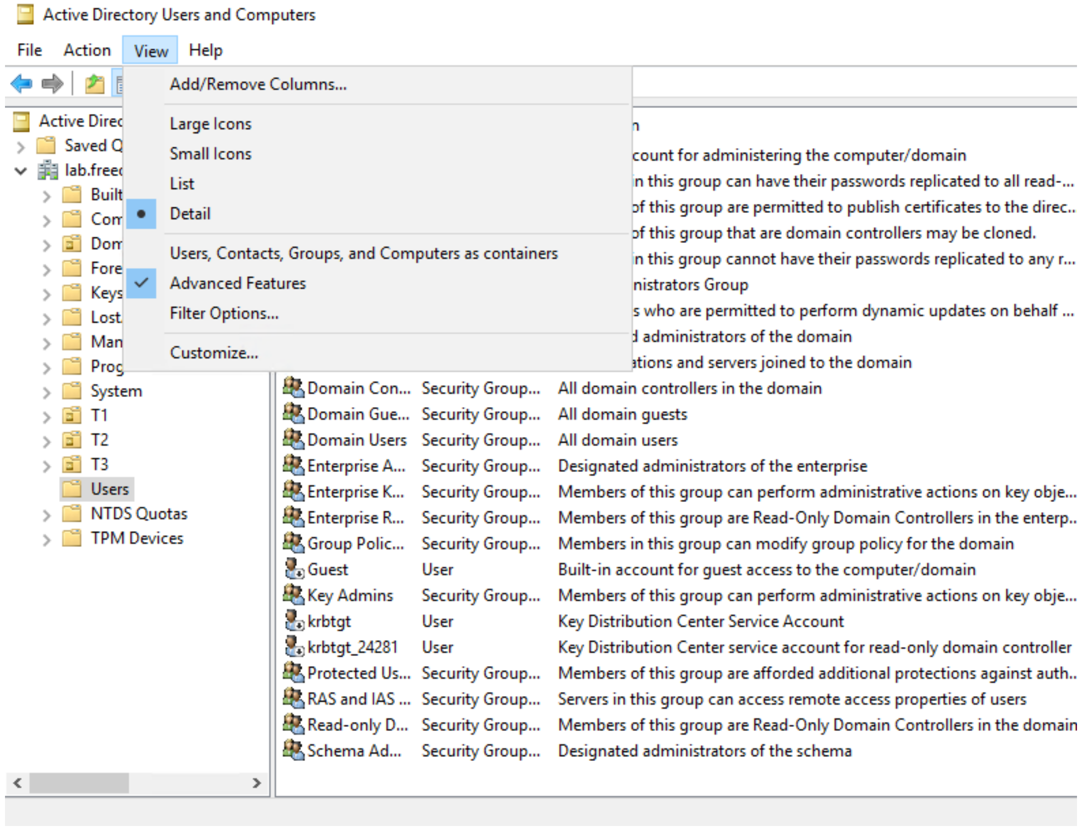
As seen in the previous example, this account is used to encrypt all the TGT’s in Active Directory.

It contains **Two** password hashes, including

- The currently password
- The previously set password

It is stored under domain users, and is visible using the advanced features of the Active Directory Management Console

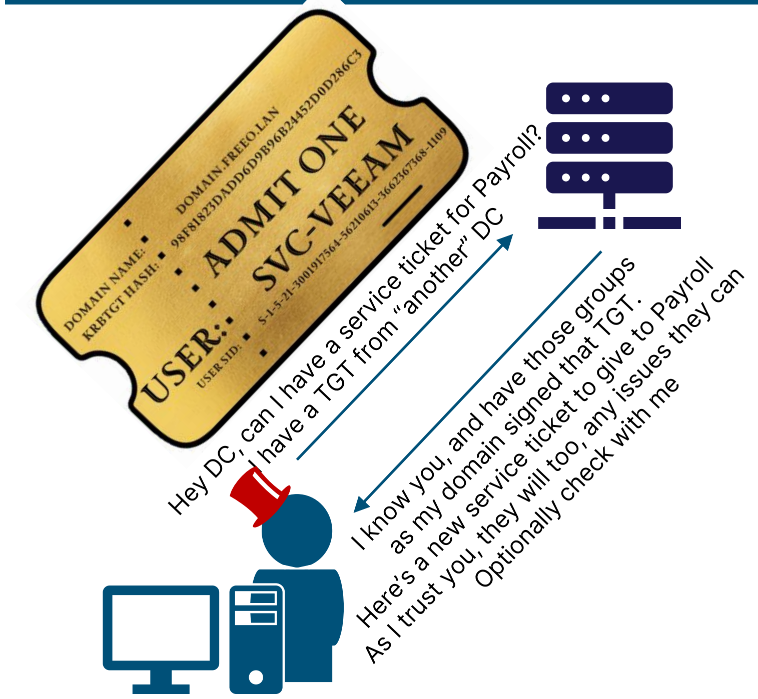
If you’re domain uses Read only Domain Controllers, you will have additional KRBTGT Accounts with *krbtgt_<number>*



n
count for administering the computer/domain
n this group can have their passwords replicated to all read-...
of this group are permitted to publish certificates to the direc..
of this group that are domain controllers may be cloned.
n this group cannot have their passwords replicated to any r...
nistrators Group
s who are permitted to perform dynamic updates on behalf ...
d administrators of the domain
ations and servers joined to the domain

Domain Con...	Security Group...	All domain controllers in the domain
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrators of the enterprise
Enterprise K...	Security Group...	Members of this group can perform administrative actions on key obje...
Enterprise R...	Security Group...	Members of this group are Read-Only Domain Controllers in the enterp..
Group Polic...	Security Group...	Members in this group can modify group policy for the domain
Guest	User	Built-in account for guest access to the computer/domain
Key Admins	Security Group...	Members of this group can perform administrative actions on key obje...
krbtgt	User	Key Distribution Center Service Account
krbtgt_24281	User	Key Distribution Center service account for read-only domain controller
Protected Us...	Security Group...	Members of this group are afforded additional protections against auth..
RAS and IAS ...	Security Group...	Servers in this group can access remote access properties of users
Read-only D...	Security Group...	Members of this group are Read-Only Domain Controllers in the domain
Schema Ad...	Security Group...	Designated administrators of the schema

Credential Theft Attacks



DOMAIN NAME: DOMAIN.FREEO.LAN
KRBTGT HASH: 98F81823DADD6D9B96B24452D0D286C3
ADMIT ONE
USER: SVC-VEEAM
USER SID: S-1-5-21-3001917564-56210613-3662367368-1109

Hey DC, can I have a service ticket for Payroll? I have a TGT from "another" DC

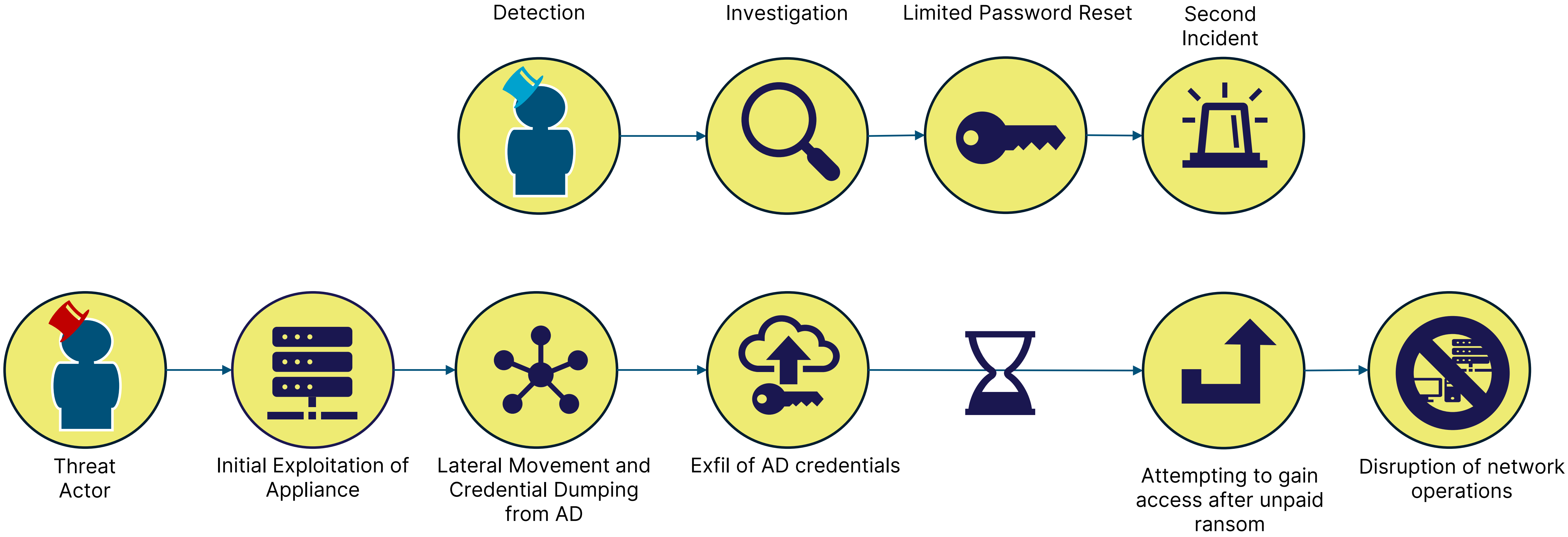
I know you, and have those groups as my domain signed that TGT. Here's a new service ticket to give to Payroll As I trust you, they will too, any issues they can Optionally check with me

Standard "User"
with a Golden TGT.
Shouldn't be getting payroll data

If a Threat Actor (**TA**) gains domain admin rights, they can get a copy of the hashes of the KRBTGT Account.

Enables the TA to impersonate *any* user when presented to the DC as its "signed" with the KRBTGT account password, (like a Certificate Authority)

Does not expire until KRBTGT is double reset



Detection

Investigation

Limited Password Reset

Second Incident

Threat Actor

Initial Exploitation of Appliance

Lateral Movement and Credential Dumping from AD

Exfil of AD credentials

Attempting to gain access after unpaid ransom

Disruption of network operations

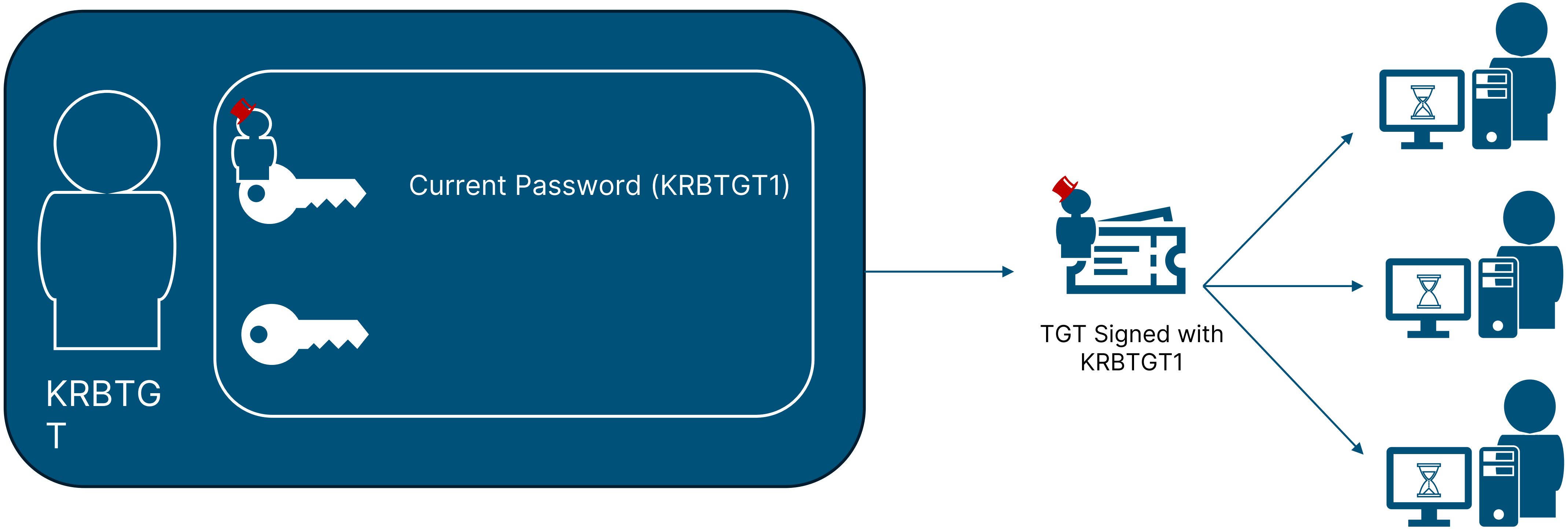
Eradication

Reset and Reset again

Reset and Wait

Reset and Reset again

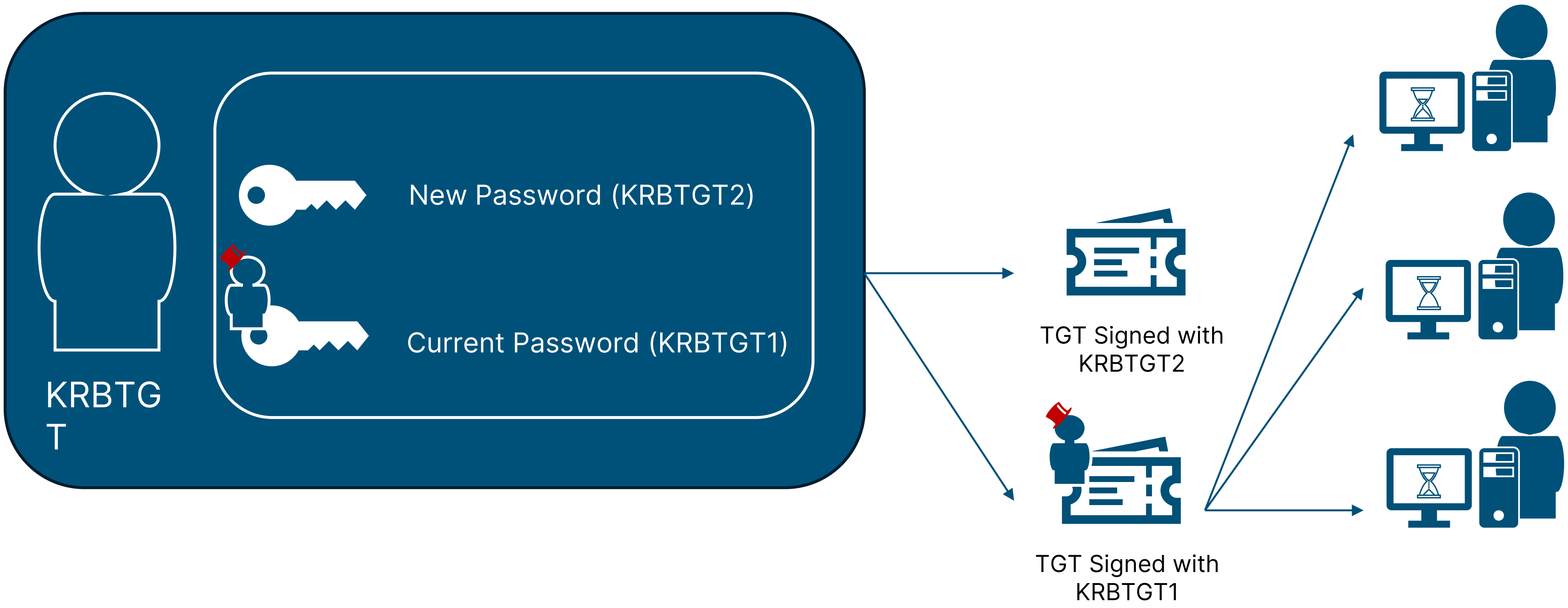
Reset and Wait

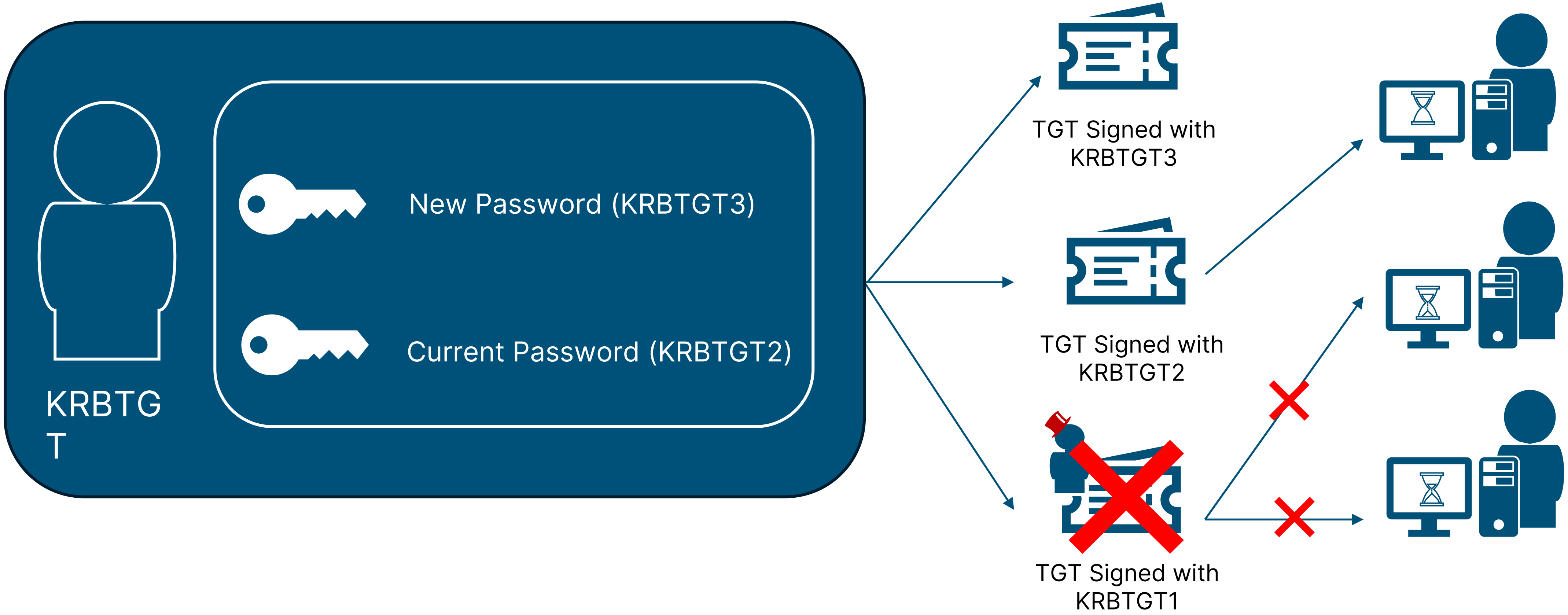


KRBTG
T

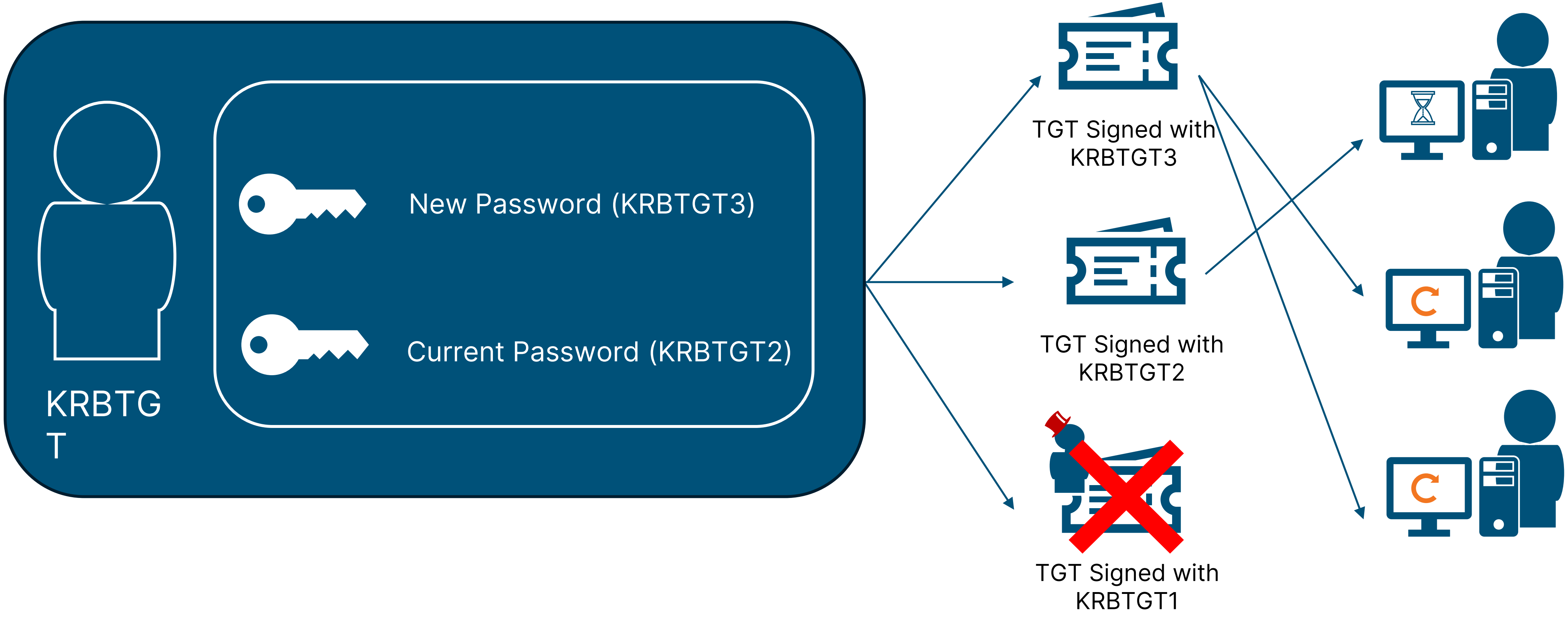
Current Password (KRBTGT1)

TGT Signed with
KRBTGT1

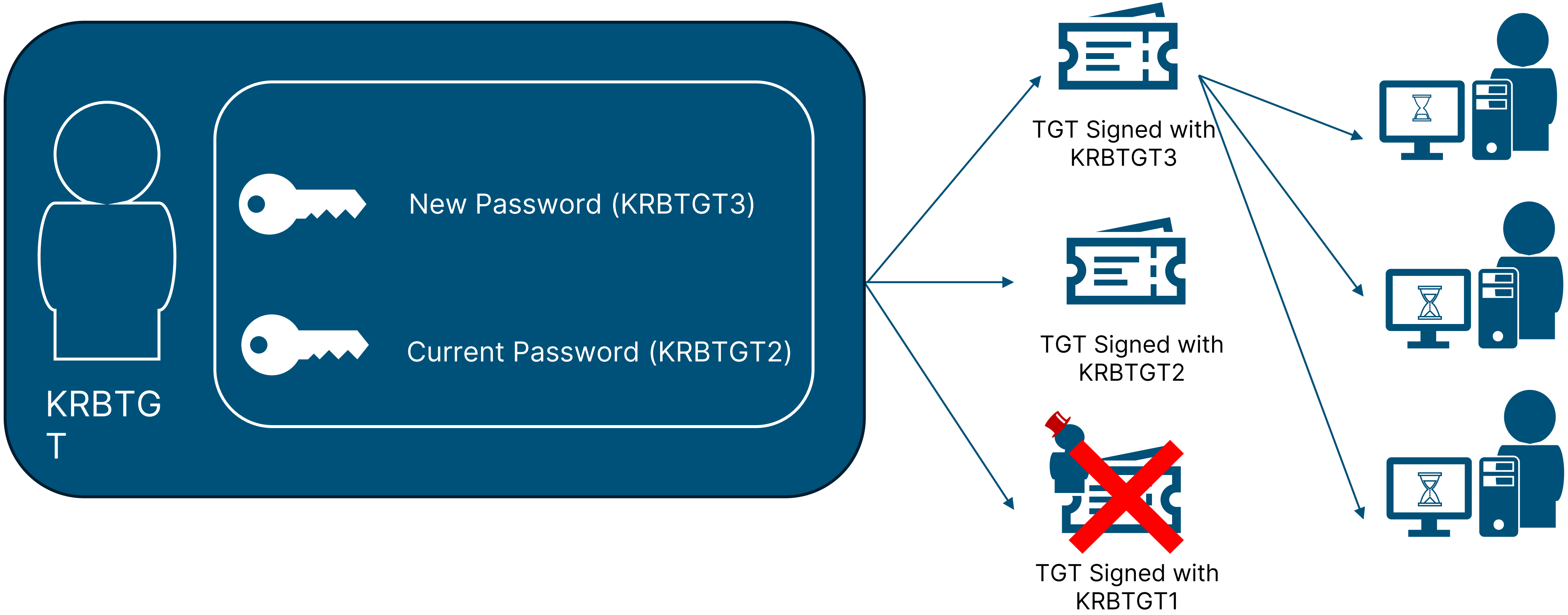

KRBTGT
New Password (KRBTGT2)
Current Password (KRBTGT1)
TGT Signed with KRBTGT2
TGT Signed with KRBTGT1



Reset and Reset Again – Second Reset

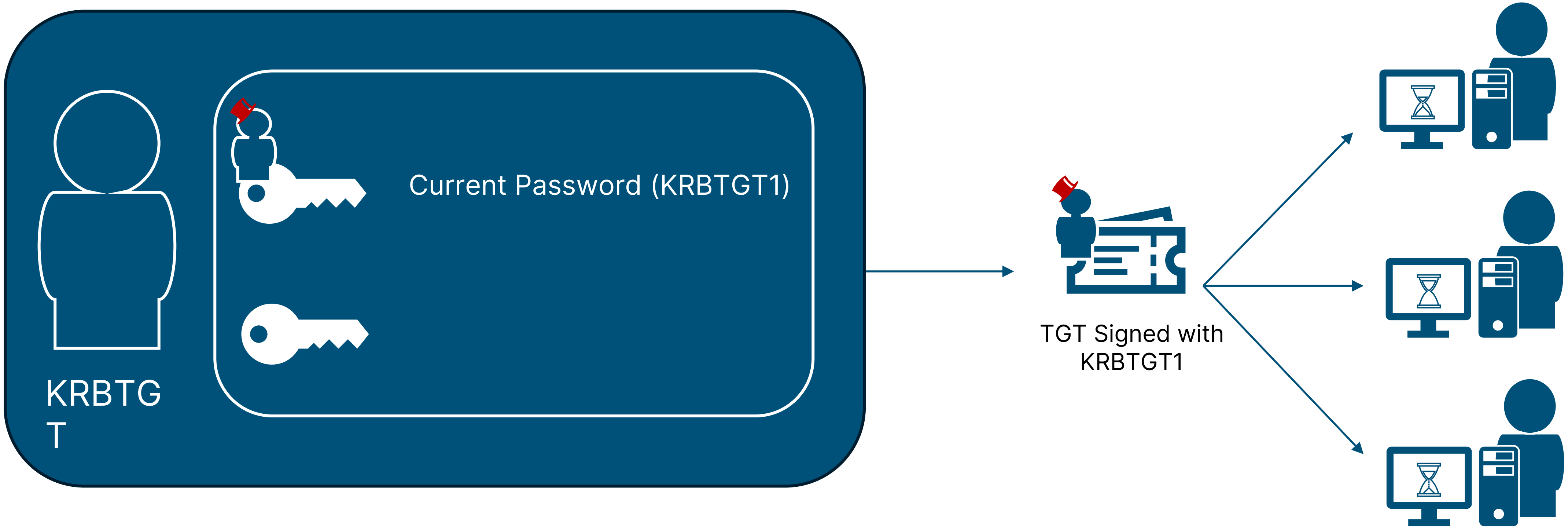


Reset and Reset Again – Second Reset



Reset and Reset again

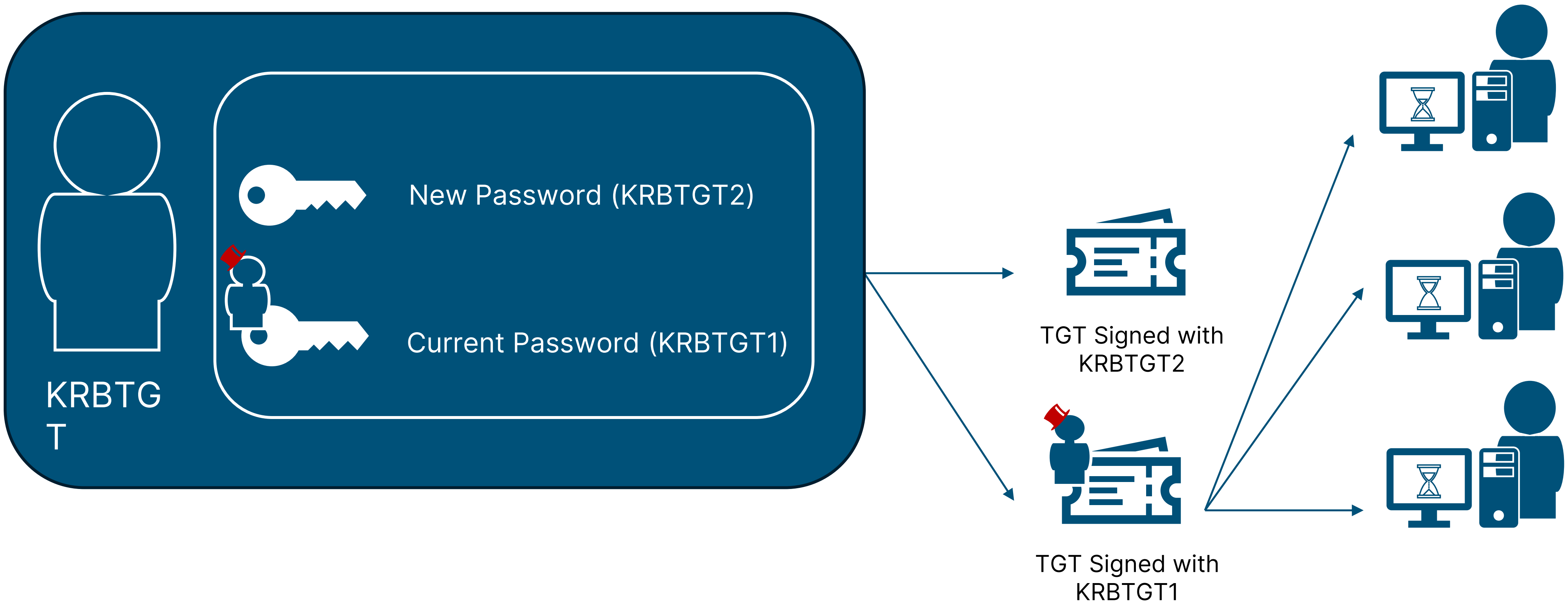
Reset and Wait



KRBTG
T

Current Password (KRBTGT1)

TGT Signed with
KRBTGT1



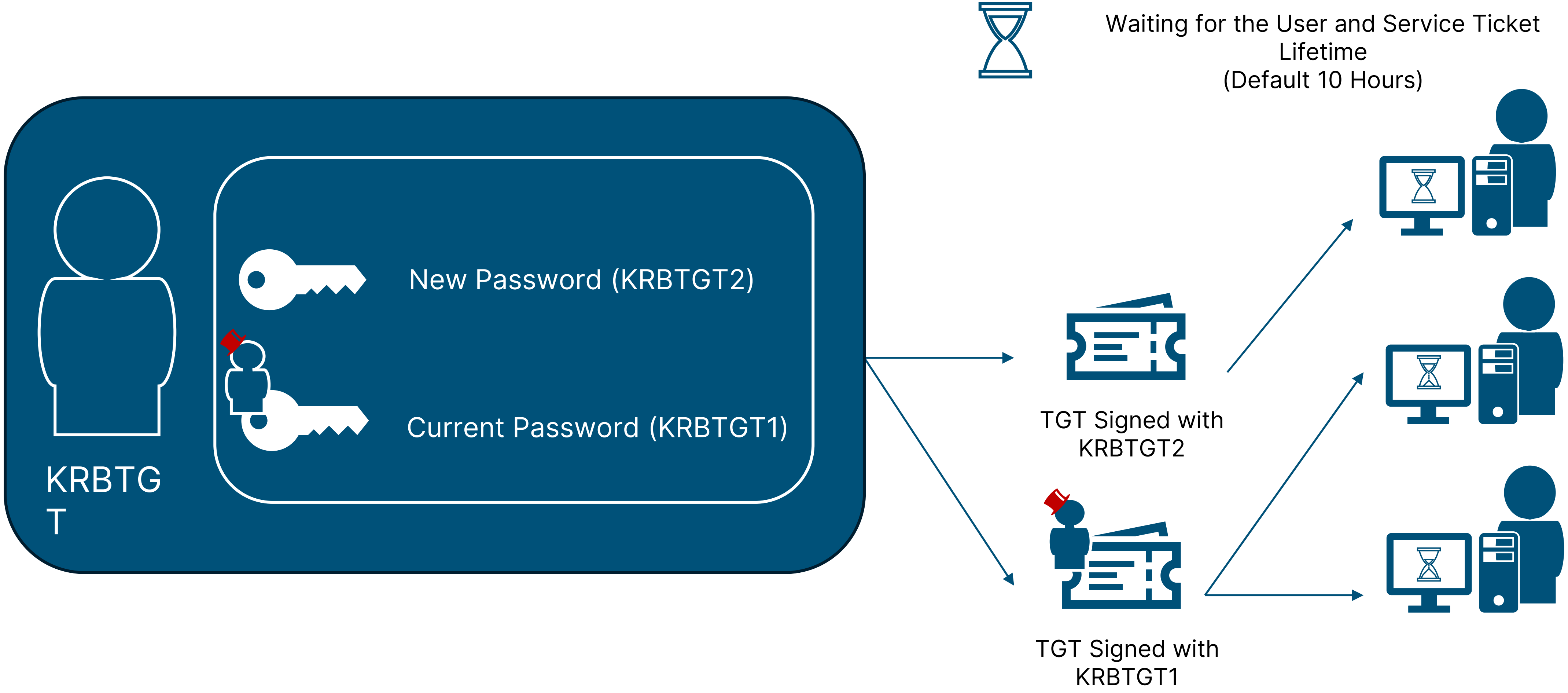
KRBTGT

New Password (KRBTGT2)

Current Password (KRBTGT1)

TGT Signed with KRBTGT2

TGT Signed with KRBTGT1



Waiting for the User and Service Ticket Lifetime
(Default 10 Hours)

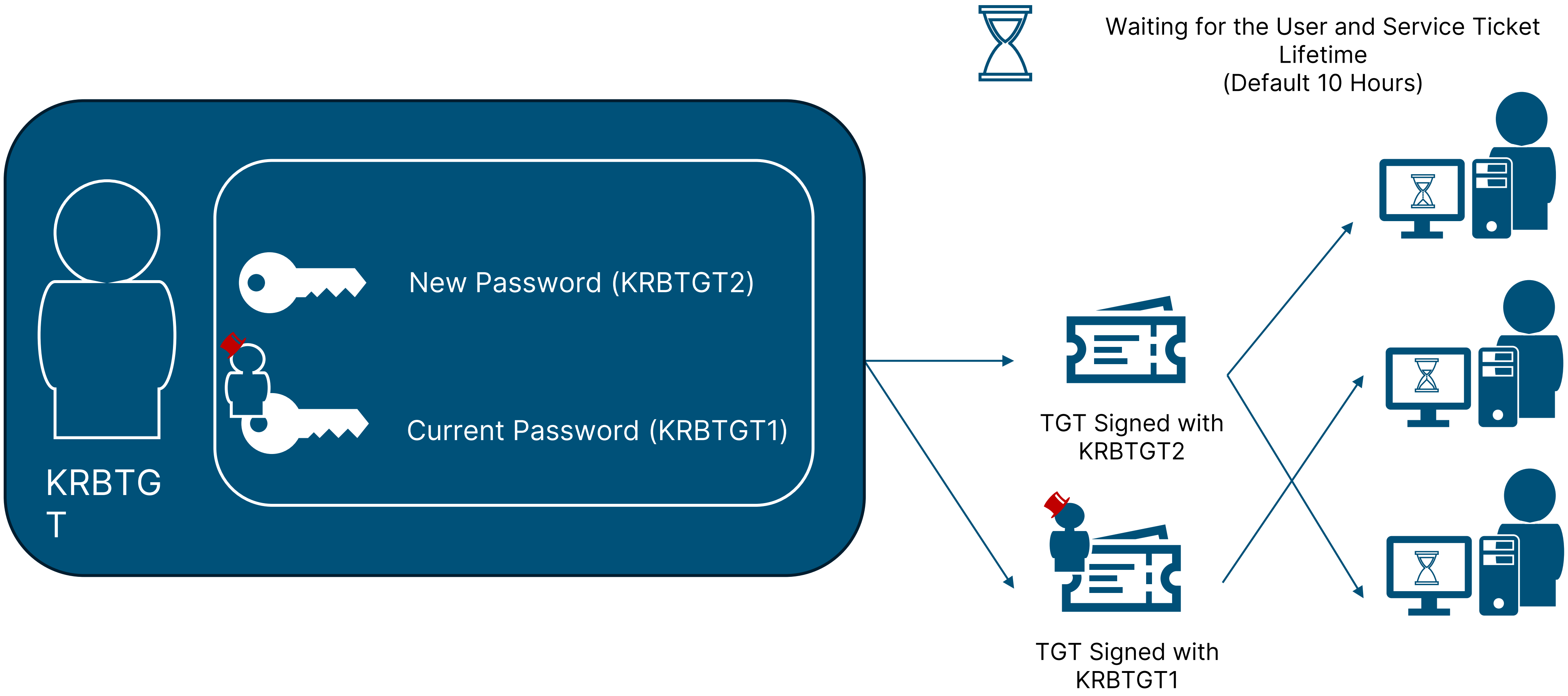
KRBTGT

New Password (KRBTGT2)

Current Password (KRBTGT1)

TGT Signed with KRBTGT2

TGT Signed with KRBTGT1



Waiting for the User and Service Ticket Lifetime
(Default 10 Hours)

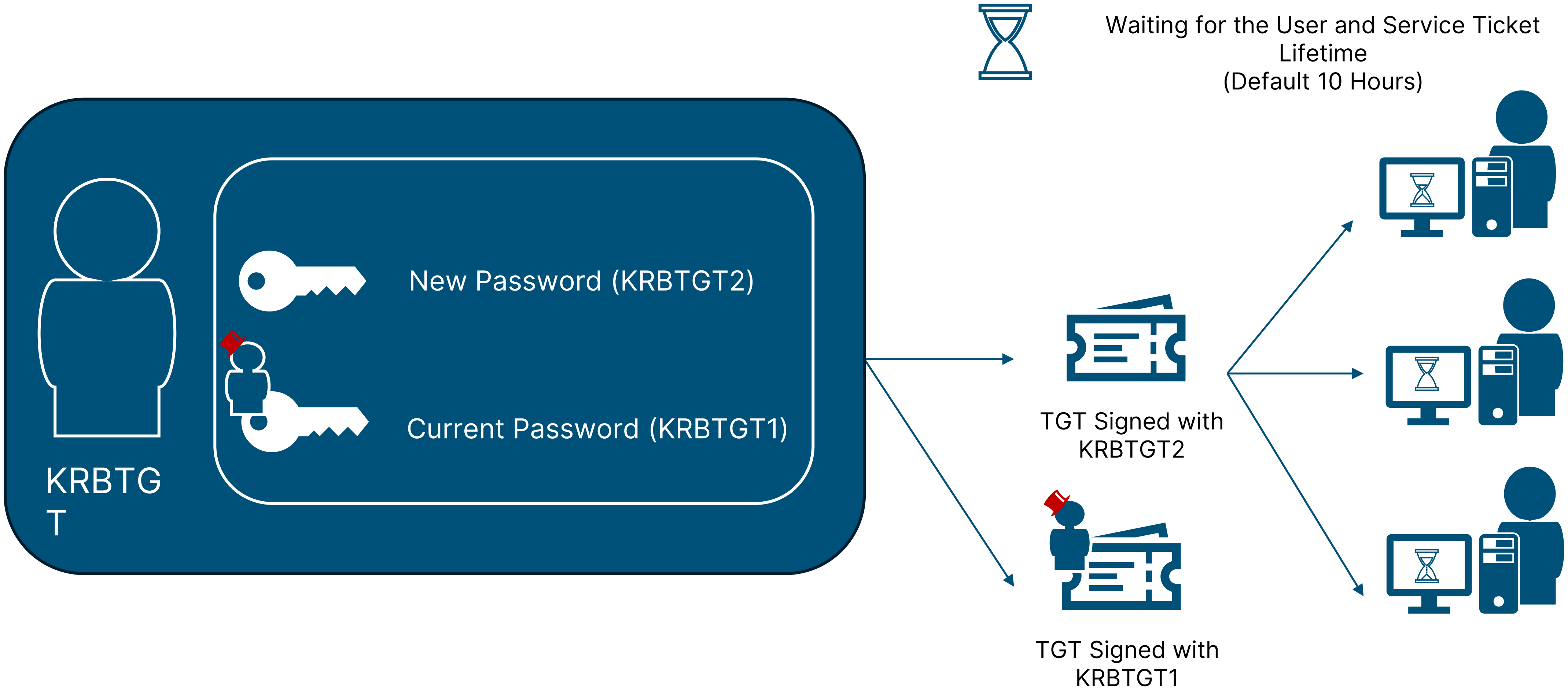
KRBTGT

New Password (KRBTGT2)

Current Password (KRBTGT1)

TGT Signed with KRBTGT2

TGT Signed with KRBTGT1



Waiting for the User and Service Ticket Lifetime
(Default 10 Hours)

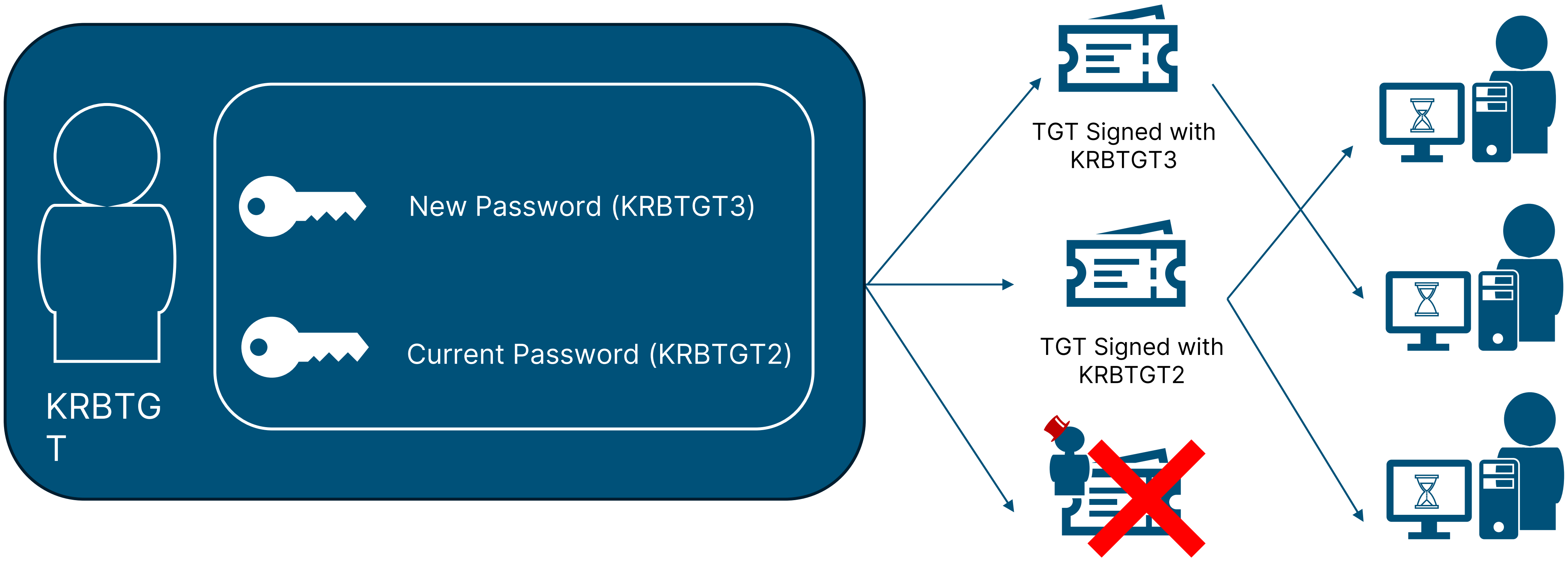
KRBTGT

New Password (KRBTGT2)

Current Password (KRBTGT1)

TGT Signed with KRBTGT2

TGT Signed with KRBTGT1



KRBTGT

New Password (KRBTGT3)

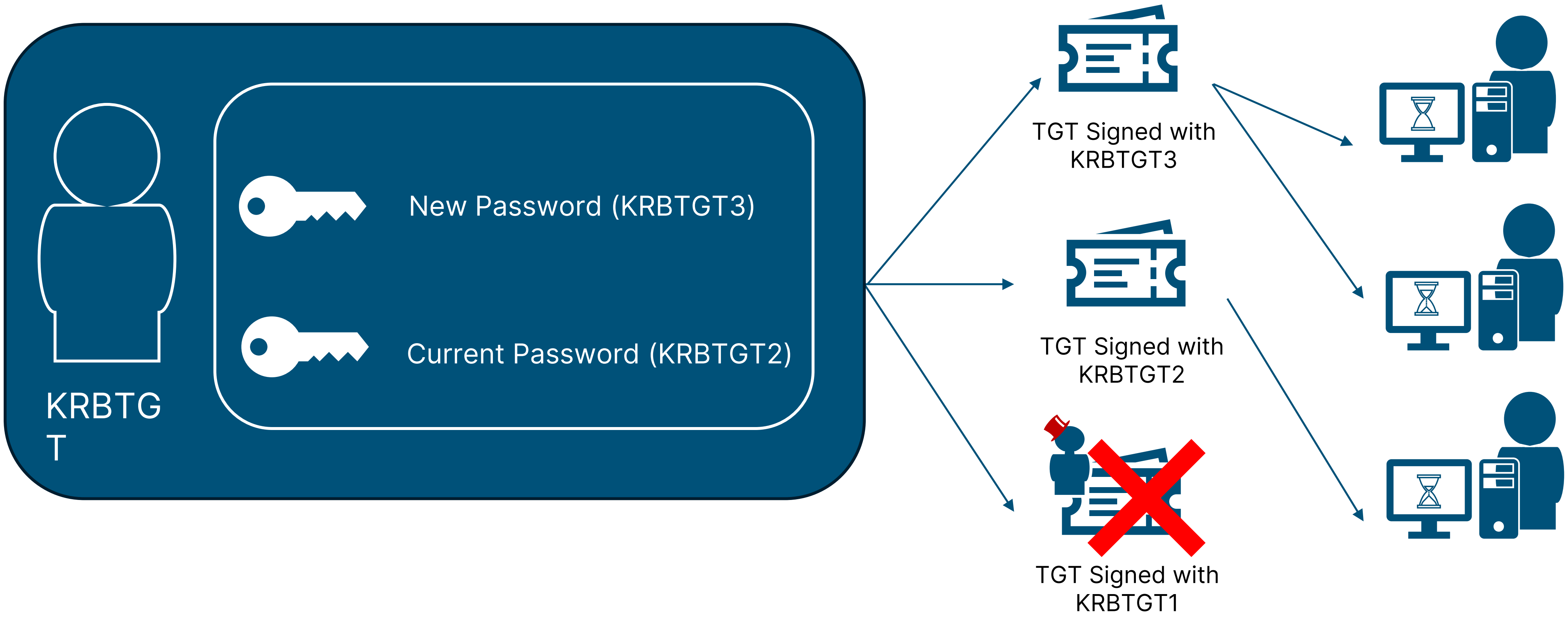
Current Password (KRBTGT2)

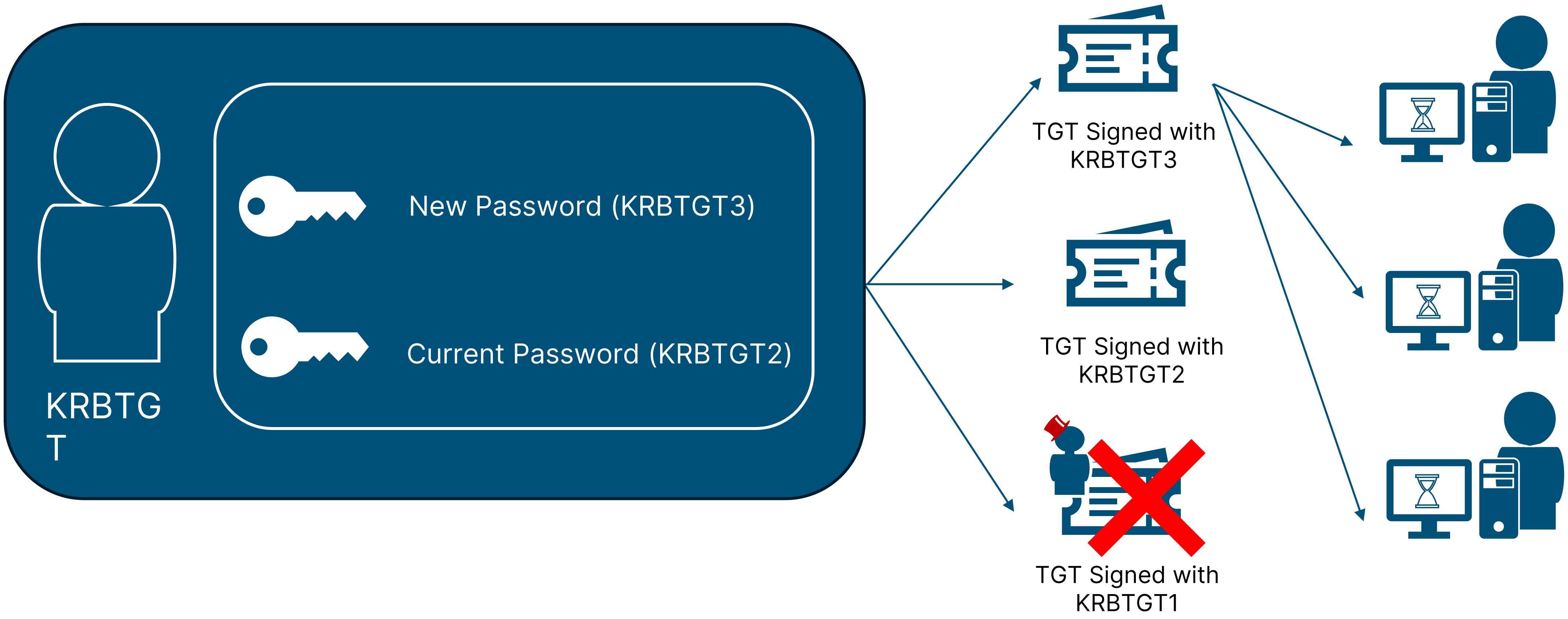
TGT Signed with KRBTGT3

TGT Signed with KRBTGT2

TGT Signed with KRBTGT1

[redacted]


KRBTGT
New Password (KRBTGT3)
Current Password (KRBTGT2)
TGT Signed with KRBTGT3
TGT Signed with KRBTGT2
TGT Signed with KRBTGT1



KRBTG
T

New Password (KRBTGT3)

Current Password (KRBTGT2)

TGT Signed with
KRBTGT3

TGT Signed with
KRBTGT2

TGT Signed with
KRBTGT1

[redacted]

Is there an active threat to my network, with no mitigating security controls?

What is the cost of downtime vs the threat of an unauthorised actor?

Is my domain healthy?

- Time
- Domain Name Services (DNS)
- Replication

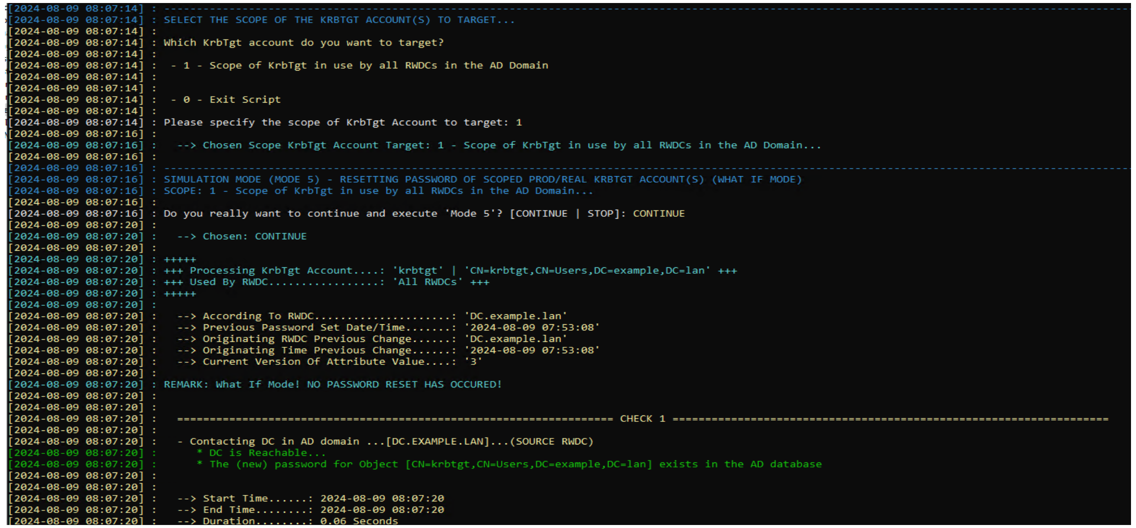
What other considerations do I have?

- Where is your Primary Domain Controller (PDC)?
- Do you have any Read Only Domain Controllers (RODC)?
- Who else has access to my domain?
- Are domains virtualised or physical?
- How can I restore if something goes wrong?
- Have I recently tested my disaster recovery plan?

Preferred:

- Free Open-Source Software (**FOSS**) provides a solution, developed by an ex-Microsoft MVP
- This script performs all AD health checks, and confirms the user wants to proceed with each step

▪https://github.com/zjorz/Public-AD-Scripts/blob/master/Reset-KrbTgt-Password-For-RWDCs-And-RODCs.ps1

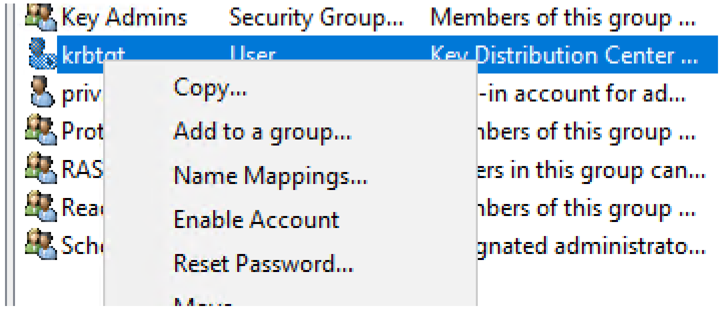


```
[2024-08-09 08:07:14] : -----------------------------------------------------------------------------------------------------------------
[2024-08-09 08:07:14] : SELECT THE SCOPE OF THE KRBTGT ACCOUNT(S) TO TARGET...
[2024-08-09 08:07:14] :
[2024-08-09 08:07:14] : Which KrbTgt account do you want to target?
[2024-08-09 08:07:14] :
[2024-08-09 08:07:14] :  - 1 - Scope of KrbTgt in use by all RWDCs in the AD Domain
[2024-08-09 08:07:14] :
[2024-08-09 08:07:14] :
[2024-08-09 08:07:14] :  - 0 - Exit Script
[2024-08-09 08:07:14] :
[2024-08-09 08:07:14] : Please specify the scope of KrbTgt Account to target: 1
[2024-08-09 08:07:16] :
[2024-08-09 08:07:16] :   --> Chosen Scope KrbTgt Account Target: 1 - Scope of KrbTgt in use by all RWDCs in the AD Domain...
[2024-08-09 08:07:16] :
[2024-08-09 08:07:16] : -----------------------------------------------------------------------------------------------------------------
[2024-08-09 08:07:16] : SIMULATION MODE (MODE 5) - RESETTING PASSWORD OF SCOPED PROD/REAL KRBTGT ACCOUNT(S) (WHAT IF MODE)
[2024-08-09 08:07:16] : SCOPE: 1 - Scope of KrbTgt in use by all RWDCs in the AD Domain...
[2024-08-09 08:07:16] :
[2024-08-09 08:07:16] : Do you really want to continue and execute 'Mode 5'? [CONTINUE | STOP]: CONTINUE
[2024-08-09 08:07:20] :
[2024-08-09 08:07:20] :   --> Chosen: CONTINUE
[2024-08-09 08:07:20] :
[2024-08-09 08:07:20] : +++++
[2024-08-09 08:07:20] : +++ Processing KrbTgt Account....: 'krbtgt' | 'CN=krbtgt,CN=Users,DC=example,DC=lan' +++
[2024-08-09 08:07:20] : +++ Used By RWDC................: 'All RWDCs' +++
[2024-08-09 08:07:20] : +++++
[2024-08-09 08:07:20] :
[2024-08-09 08:07:20] :   --> According To RWDC.....................: 'DC.example.lan'
[2024-08-09 08:07:20] :   --> Previous Password Set Date/Time.......: '2024-08-09 07:53:08'
[2024-08-09 08:07:20] :   --> Originating RWDC Previous Change......: 'DC.example.lan'
[2024-08-09 08:07:20] :   --> Originating Time Previous Change......: '2024-08-09 07:53:08'
[2024-08-09 08:07:20] :   --> Current Version Of Attribute Value....: '3'
[2024-08-09 08:07:20] :
[2024-08-09 08:07:20] : REMARK: What If Mode! NO PASSWORD RESET HAS OCCURED!
[2024-08-09 08:07:20] :
[2024-08-09 08:07:20] :
[2024-08-09 08:07:20] :   =================================================================== CHECK 1 ===================================================================
[2024-08-09 08:07:20] :
[2024-08-09 08:07:20] :   - Contacting DC in AD domain ...[DC.EXAMPLE.LAN]...(SOURCE RWDC)
[2024-08-09 08:07:20] :      * DC is Reachable...
[2024-08-09 08:07:20] :      * The (new) password for Object [CN=krbtgt,CN=Users,DC=example,DC=lan] exists in the AD database
[2024-08-09 08:07:20] :
[2024-08-09 08:07:20] :
[2024-08-09 08:07:20] :   --> Start Time......: 2024-08-09 08:07:20
[2024-08-09 08:07:20] :   --> End Time........: 2024-08-09 08:07:20
[2024-08-09 08:07:20] :   --> Duration........: 0.06 Seconds
```

Alternative:

- Login to your domain controller, and perform health checks manually
- Open Active Directory Users and Computers (**ADUC**), and select View, Advanced Features
- Find the KRBTGT account under the default users OU
- Right click and reset password

▪Note: Microsoft KB2549833 states that the KRBTGT password is set automatically to a random string when entered.



Key Admins Security Group... Members of this group ...
krbtgt User Key Distribution Center ...
priv -in account for ad...
Prot nbers of this group ...
RAS ers in this group can...
Rea nbers of this group ...
Sch gnated administrato...

[redacted]

If a TA had access to the KRBTGT hash, its highly likely they had access to all the credentials for the domain

- Reset *ALL* domain passwords:

Enterprise and Domain Admins

Exchange/Sharepoint Administrators

Service Accounts

Domain Users*

Continue monitoring for unusual activity

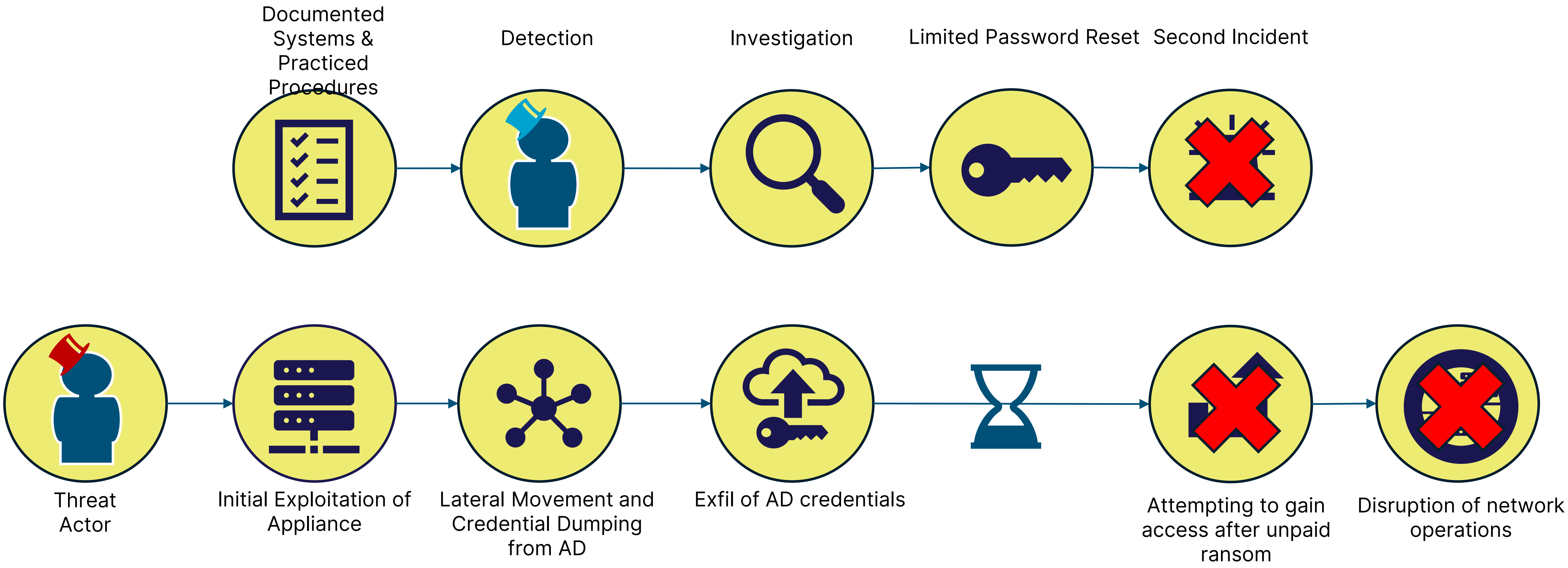
Lessons Learned from the Field

Check your domains documentation

Test and exercise KRBTGT resets before an Incident

Update credential theft playbooks

Enable agile change management


Documented Systems & Practiced Procedures
Detection
Investigation
Limited Password Reset
Second Incident
Threat Actor
Initial Exploitation of Appliance
Lateral Movement and Credential Dumping from AD
Exfil of AD credentials
Attempting to gain access after unpaid ransom
Disruption of network operations

[MS-KILE]: Kerberos Network Authentication Service (V5) Synopsis | Microsoft Learn
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-kile/b4af186e-b2ff-43f9-b18e-eedb366abf13

Kerberos Policy - Windows Security | Microsoft Learn - https://learn.microsoft.com/er
us/windows/security/threat-protection/security-policy-settings/kerberos-policy

Kerberos & KRBTGT: Active Directory’s Domain Kerberos Service Account – Active Directory Security (adsecurity.org) - https://adsecurity.org/?p=483

Detecting Forged Kerberos Ticket (Golden Ticket & Silver Ticket) Use in Active Directory – Active Directory Security (adsecurity.org) - https://adsecurity.org/?p=1515

AD Forest Recovery - Resetting the krbtgt password | Microsoft Learn -
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/forest-recovery-guide/ad-forest-recovery-reset-the-krbtgt-password

KRBTGT Password Reset Script - https://github.com/zjorz/Public-AD-Scripts/blob/master/Reset-KrbTgt-Password-For-RWDCs-And-RODCs.ps1

DCTPRESENTATION.GITHUB.IO

Adelaide Agenda

TIME	TOPIC
09:15 – 09:45 AM	**Welcome & Introduction** MJ Shoer, Chief Community Officer, CompTIA
09:45 – 10:00 AM	**Privacy Act Changes Impacting Your Business** David Norris, Managing Director, Nortec IT, Dean Calvert, Founder, Calvert Technologies
10:00 – 10:30 AM	**State of Cybersecurity.** David Norris, Managing Director, Nortec IT
10:30 – 11:00 AM	**MORNING TEA & NETWORKING BREAK**
11:00 – 11:30 AM	**Securing Active Directory:** KRBTGT Resets After Credential Theft. Samuel Freeman, Senior Investigator DFIR, CyberCX
11:30 AM – 12:30 PM	**Risk Management for your business. Part 1.** Wayne Selk, VP Cybersecurity Programs, CompTIA
12:30 – 12:35 PM	**QUICK BREAK**
12:35 – 1:00 PM	**State of the Channel, with ANZ Perspectives.** Maria Armstrong, Manager of Academy APAC, Pax8
1:00 – 2:00 PM	**LUNCH & NETWORKING**

WE ARE THE

CompTIA®

Community

RISK MANAGEMENT FOR YOUR BUSINESS..

WAYNE SELK, VP CYBERSECURITY PROGRAMS, COMPTIA

Risk Management Course

A CompTIA Cybersecurity Trustmark Series

CompTIA CYBERSECURITY Programs

Understanding Business Risk

Part 1

What is this Course?

Cybersecurity Trustmark Risk Management Course

- This course is an immersive dive into the world of business risk
- Each Part is approximately ONE Hour
- In the five-part series, you will learn to:
  - Understand Business Risk – Part 1
  - Operationalize Your Risk – Part 2
  - Help Your Clients Understand Their Risk – Part 3
  - Create a Strategy for Risk – Part 4
  - Create Opportunity for Risk – Part 5

What Will I Be Learning

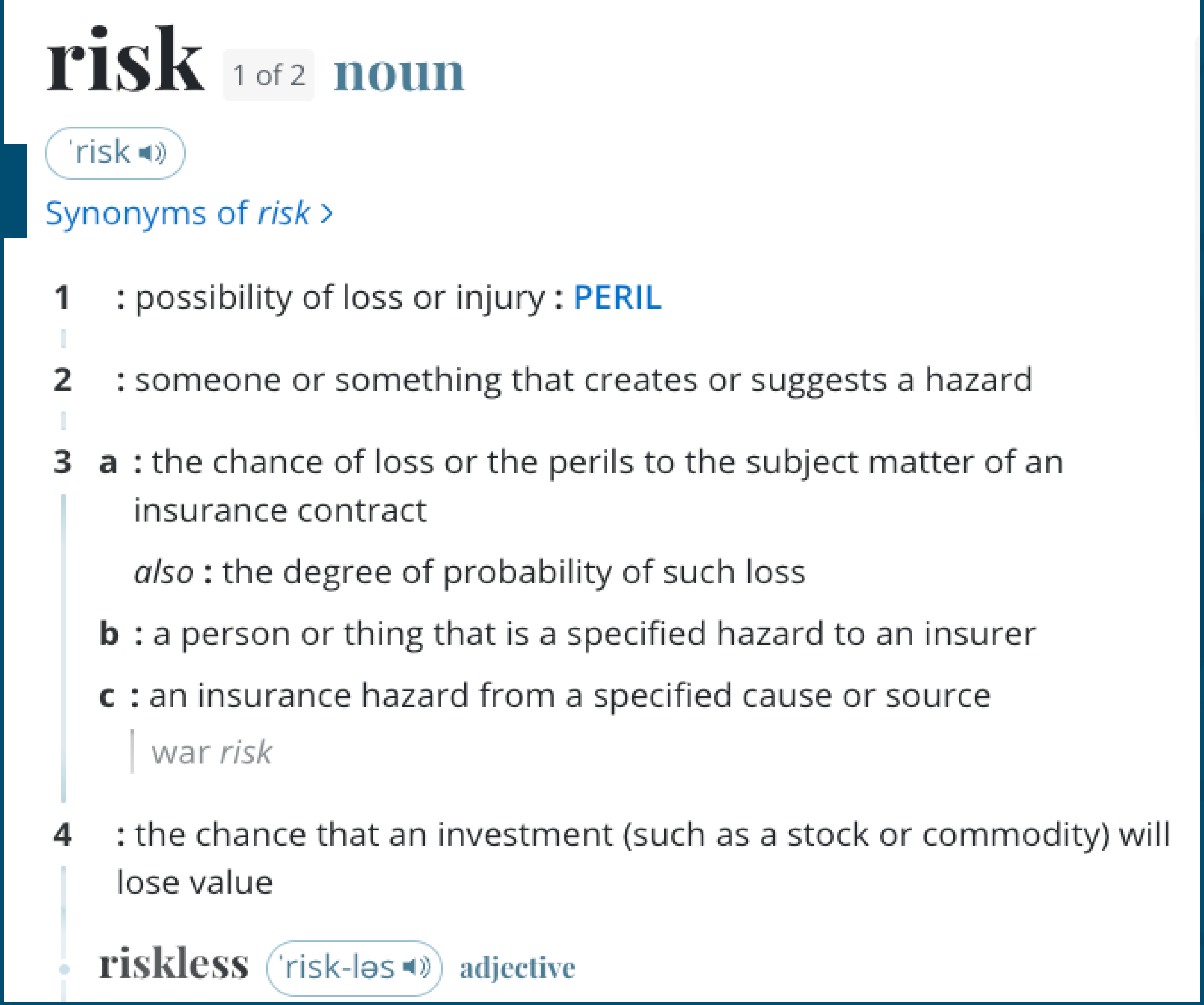
Agenda

- Risk - Defined
- Identifying Risk
- Business Impact Analysis (BIA)
- Creating a Dashboard
- Learning to Live With Risk
- Getting Ready to Operationalize Risk

Any corporation that doesn't recognize its Achilles' heel is fated to die because of it.

Source: Harvard Business Review Article, "The Six Mistakes Executives Makes in Risk Management, October 2009 Magazine

Risk - Defined



risk 1 of 2 **noun**

ˈrisk

Synonyms of *risk* ›

1 : possibility of loss or injury : PERIL

2 : someone or something that creates or suggests a hazard

3 **a** : the chance of loss or the perils to the subject matter of an insurance contract

also : the degree of probability of such loss

b : a person or thing that is a specified hazard to an insurer

c : an insurance hazard from a specified cause or source

war *risk*

4 : the chance that an investment (such as a stock or commodity) will lose value

riskless ˈrisk-ləs **adjective**

CompTIA CYBERSECURITY Programs

Business Risk - Defined

The Hartford defines business risk as:

“anything that could impact your company’s finances”

Inherent vs Residual Risk

Inherent Risk – The amount of risk that exists in the absence of controls

Residual Risk – The amount of risk remaining which exists after controls are applied

Identifying Risk

BRAINSTORMING

THINK LIKE A PESSIMIST

ASK EMPLOYEES

You’ve Identified it, Now What…

- Identifying risk(s) is just the beginning
- You need to be able to turn what you learned into something useful
- Start with just a small (or what might appear small) item
- Develop a Business Impact Analysis or BIA

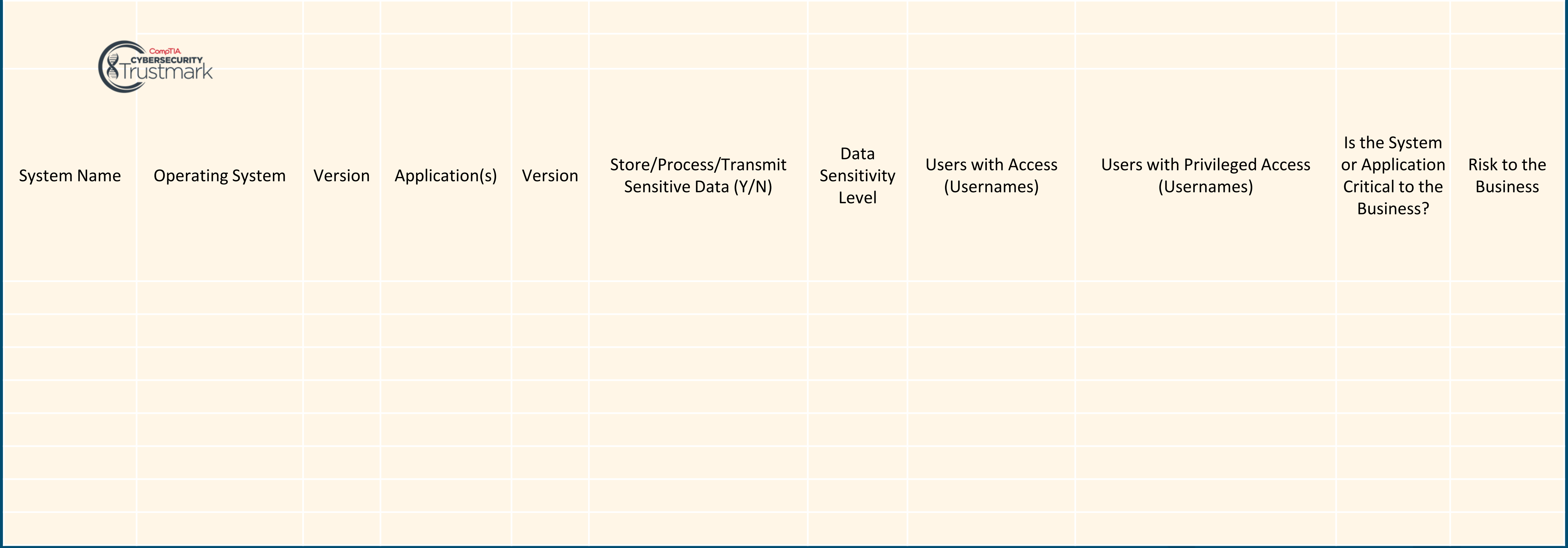
Asset Inventory

Most important step…

- Inventory all your assets will help prioritize containment and response
    - System
        - Application
            - Data Sensitivity
        - Application (if more than one on a system)
            - Data Sensitivity
        - Who has Access
            - What level of access
        - Determination of Criticality
            - Should be based upon the data sensitivity
        - Determination of Risk to the Business
            - Low, Medium, High

Create an Asset Inventory

Microsoft Excel Worksheet



System Name	Operating System	Version	Application(s)	Version	Store/Process/Transmit Sensitive Data (Y/N)	Data Sensitivity Level	Users with Access (Usernames)	Users with Privileged Access (Usernames)	Is the System or Application Critical to the Business?	Risk to the Business

The Business Impact Analysis - Defined

“The BIA predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies.”

CompTIA CYBERSECURITY Programs

Source: https://www.ready.gov/business-impact-analysis

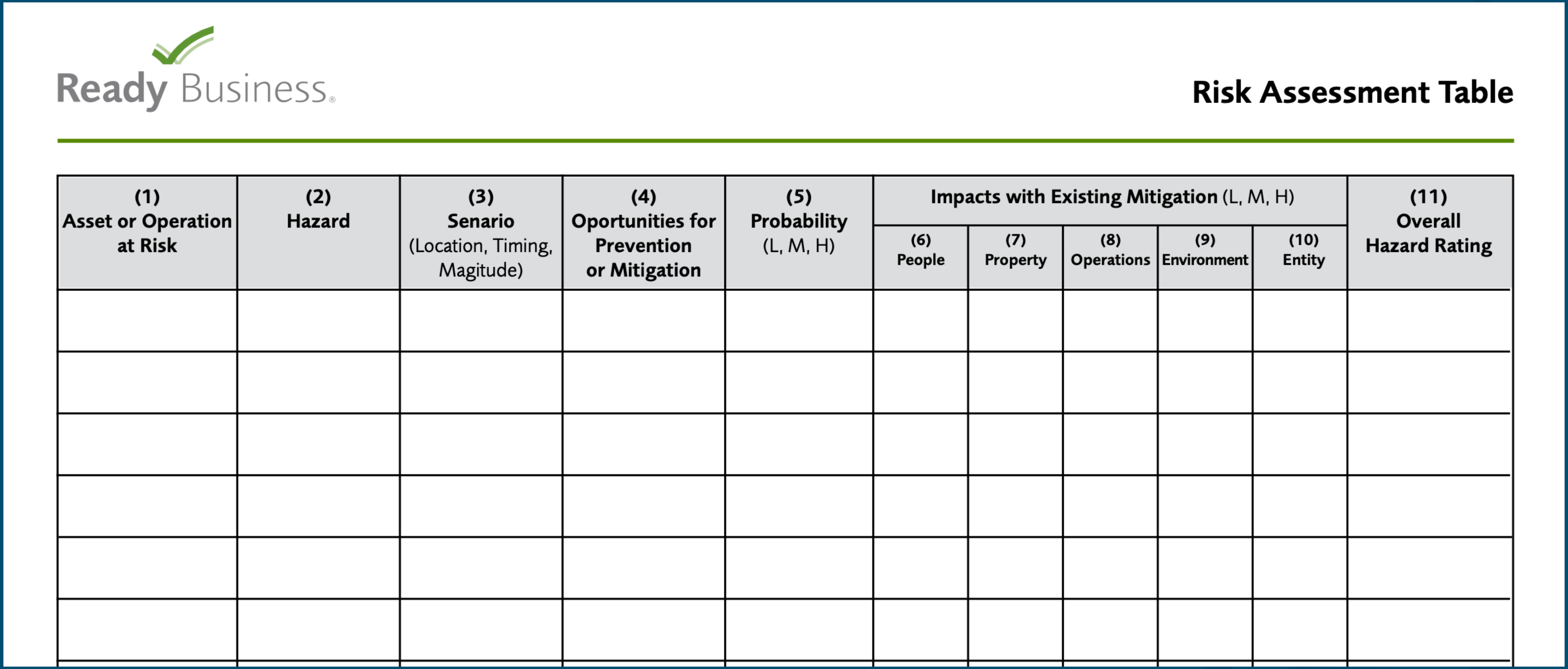
Four Sections to the BIA

- Consider the Impact
- Timing and Duration of the Disruption(s)
- Conducting the BIA itself
- Producing the BIA Report

Business Disruption Scenarios

- Physical damage to buildings
- Damage to or breakdown of critical equipment
- Interruption of the Supply Chain
- Utility Outage
- Damage to, loss or corruption of information technology including voice and data communications, servers, computers, operating systems, applications, and data
- Absenteeism of Critical Staff

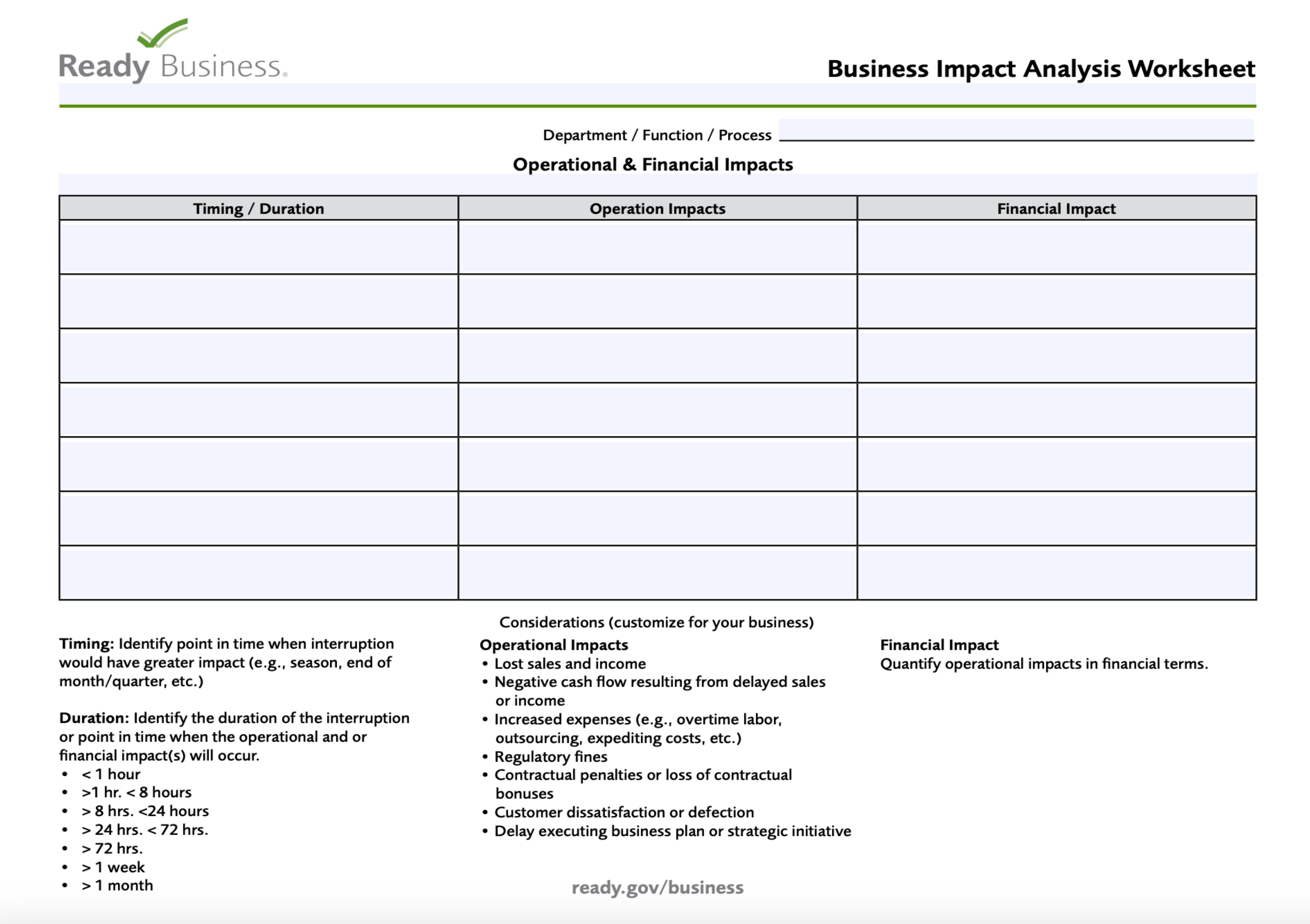
Microsoft Excel Worksheet



Ready Business®

Risk Assessment Table

(1) Asset or Operation at Risk	(2) Hazard	(3) Senario (Location, Timing, Magitude)	(4) Oportunities for Prevention or Mitigation	(5) Probability (L, M, H)	**Impacts with Existing Mitigation** (L, M, H)					(11) Overall Hazard Rating
					(6) People	(7) Property	(8) Operations	(9) Environment	(10) Entity	



Ready Business.

Business Impact Analysis Worksheet

Department / Function / Process ______________________

Operational & Financial Impacts

Timing / Duration	Operation Impacts	Financial Impact

Considerations (customize for your business)

Timing: Identify point in time when interruption would have greater impact (e.g., season, end of month/quarter, etc.)

Duration: Identify the duration of the interruption or point in time when the operational and or financial impact(s) will occur.

- < 1 hour
- >1 hr. < 8 hours
- > 8 hrs. <24 hours
- > 24 hrs. < 72 hrs.
- > 72 hrs.
- > 1 week
- > 1 month

Operational Impacts

- Lost sales and income
- Negative cash flow resulting from delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay executing business plan or strategic initiative

Financial Impact

Quantify operational impacts in financial terms.

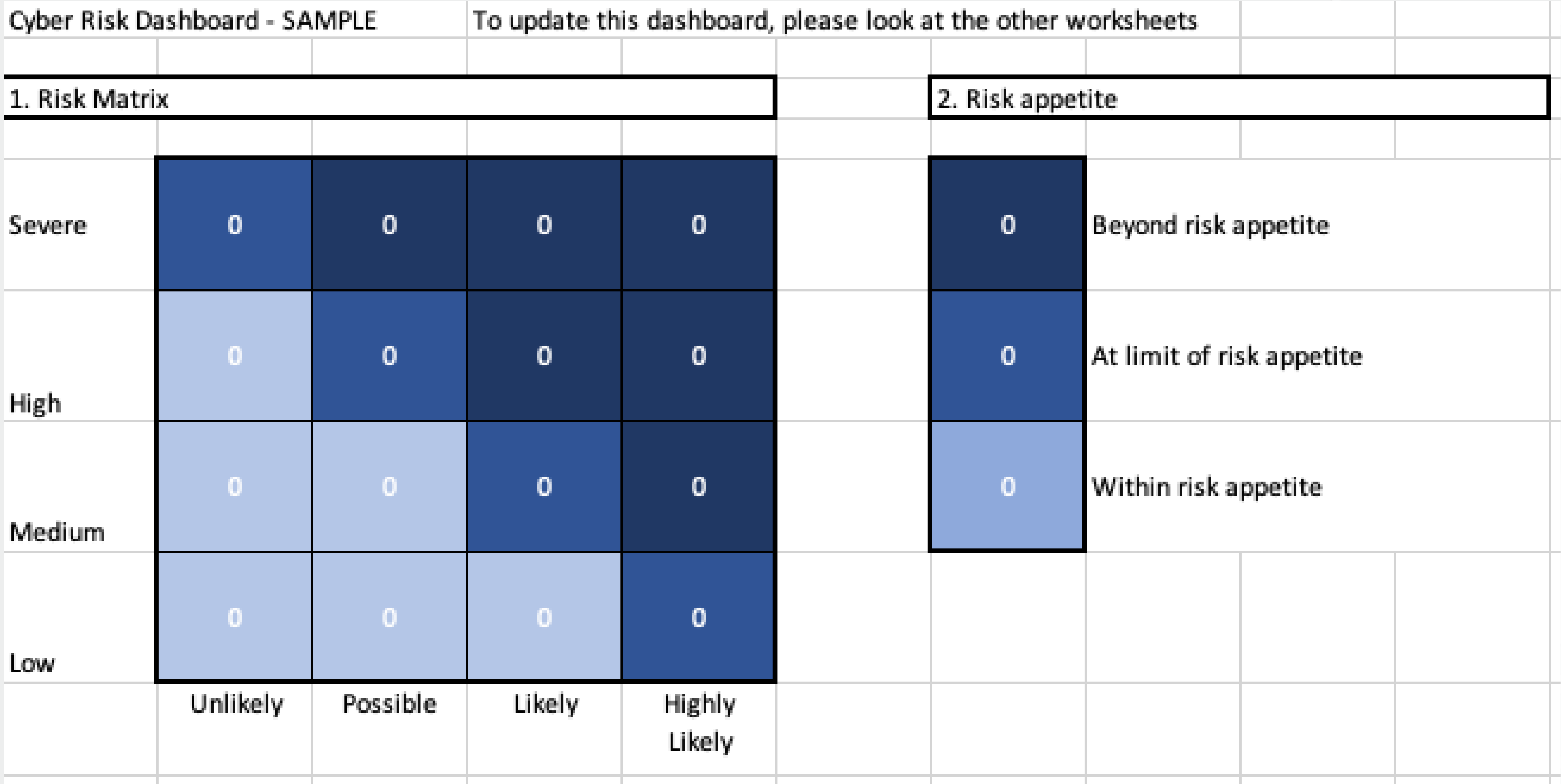
ready.gov/business

Microsoft Excel Worksheet

CompTIA CYBERSECURITY Programs

Measuring for Success

Microsoft Excel Worksheet



Cyber Risk Dashboard - SAMPLE   To update this dashboard, please look at the other worksheets

1. Risk Matrix

	Unlikely	Possible	Likely	Highly Likely
Severe	0	0	0	0
High	0	0	0	0
Medium	0	0	0	0
Low	0	0	0	0

2. Risk appetite

0	Beyond risk appetite
0	At limit of risk appetite
0	Within risk appetite

Dashboard Uniqueness

- Threats impacting you or your clients
- Overview of recent Cyber incidents, incident development, and key countermeasures taken
- Security Awareness Training Completion Percentage
- Risk Appetite is a constantly changing number
- Risk is subjective

Physical and Emotional Challenges

- Staffing shortages and limited experience increase stress and strain
- Cyber criminals tend to launch during off-peak hours
- Not uncommon to feel as though you are at fault
- Missteps during incident response lead to more stress

Do Not De-Sensitize – Do Not Panic Either

- Have a documented incident response plan
- Practice the plan, have a “hot wash”, update the plan, repeat
- Invest in talent when it makes sense
- Add an Employee Assistance Program (EAP) to your health benefits
- Mistakes happen, create a culture where reporting is not demonized

What’s Next?

Part 2

- What is Business Risk
- Seven Types of Business Risk
- Uncovering Risk
- A “Methodology”
- Ensure Alignment

Homework – Prepare for Part 2

- Create a BIA for a department or a System
- Create a dashboard
- Create a process for reviewing Risk with the team

Adelaide Agenda

CompTIA Community

TIME	TOPIC
09:15 – 09:45 AM	**Welcome & Introduction** MJ Shoer, Chief Community Officer, CompTIA
09:45 – 10:00 AM	**Privacy Act Changes Impacting Your Business** David Norris, Managing Director, Nortec IT, Dean Calvert, Founder, Calvert Technologies
10:00 – 10:30 AM	**State of Cybersecurity.** David Norris, Managing Director, Nortec IT
10:30 – 11:00 AM	**MORNING TEA & NETWORKING BREAK**
11:00 – 11:30 AM	**Securing Active Directory:** KRBTGT Resets After Credential Theft. Samuel Freeman, Senior Investigator DFIR, CyberCX
11:30 AM – 12:30 PM	**Risk Management for your business. Part 1.** Wayne Selk, VP Cybersecurity Programs, CompTIA
12:30 – 12:35 PM	**QUICK BREAK**
12:35 – 1:00 PM	**State of the Channel, with ANZ Perspectives.** Maria Armstrong, Manager of Academy APAC, Pax8
1:00 – 2:00 PM	**LUNCH & NETWORKING**

WE ARE THE CompTIA® Community

12:30 - 12:35 PM

QUICK BREAK

Adelaide Agenda

CompTIA Community

TIME	TOPIC
09:15 – 09:45 AM	**Welcome & Introduction** MJ Shoer, Chief Community Officer, CompTIA
09:45 – 10:00 AM	**Privacy Act Changes Impacting Your Business** David Norris, Managing Director, Nortec IT, Dean Calvert, Founder, Calvert Technologies
10:00 – 10:30 AM	**State of Cybersecurity.** David Norris, Managing Director, Nortec IT
10:30 – 11:00 AM	**MORNING TEA & NETWORKING BREAK**
11:00 – 11:30 AM	**Securing Active Directory:** KRBTGT Resets After Credential Theft. Samuel Freeman, Senior Investigator DFIR, CyberCX
11:30 AM – 12:30 PM	**Risk Management for your business. Part 1.** Wayne Selk, VP Cybersecurity Programs, CompTIA
12:30 – 12:35 PM	**QUICK BREAK**
12:35 – 1:00 PM	**State of the Channel, with ANZ Perspectives.** Maria Armstrong, Manager of Academy APAC, Pax8
1:00 – 2:00 PM	**LUNCH & NETWORKING**

WE ARE THE

CompTIA

Community

12:05pm-12:55pm

STATE OF THE CHANNEL, WITH ANZ PERSPECTIVES.

Maria Armstrong, Manager of Academy APAC, Pax8

CompTIA

State of the Channel 2024
ANZ

Key State of the Channel Stats

$1.5 trillion

Estimated spending on IT services globally in 2024, an 8.7% growth rate year-over-year to place as top segment of technology spending for the first time.

(Source: Gartner, January 2024 projection)

58%
of ANZ channel firms say their business is in better shape today than it was two years ago

49%
of ANZ channel firms say competition and pricing pressure concern them most as top inhibitors to revenue growth and profitability

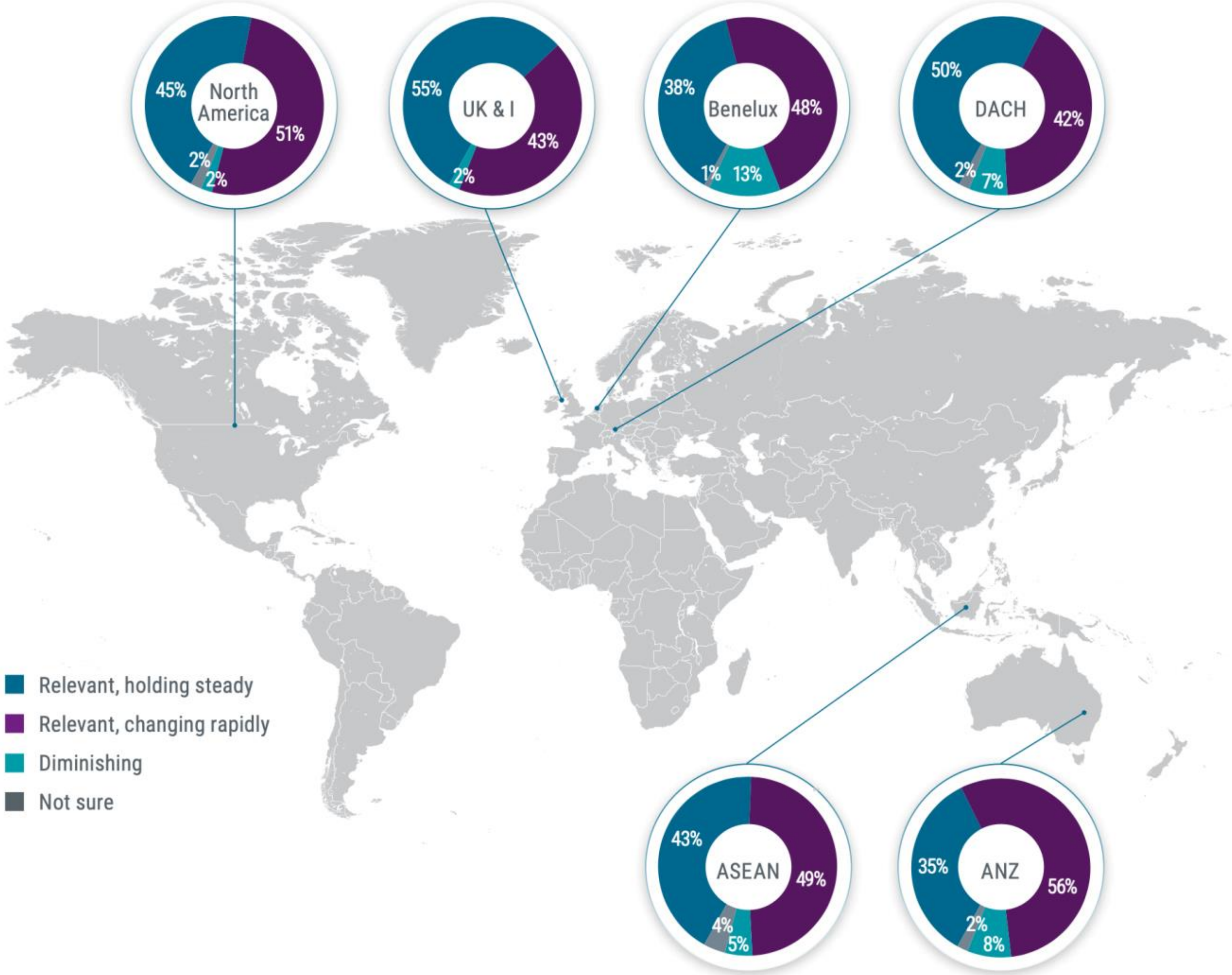
44%
of ANZ channel firms say they plan to sell generative AI-based solutions to customers in 2024

46%
of ANZ channel firms cited training and certification as the main remedy for improving business skills

30%
of ANZ channel firms say they participate in zero to four partner programs today

26%
of ANZ channel firms describe their company as “expert” in terms of general business acumen

Global Channel Outlook



Source: CompTIA 2024 State of the Channel survey | n=1042 international respondents

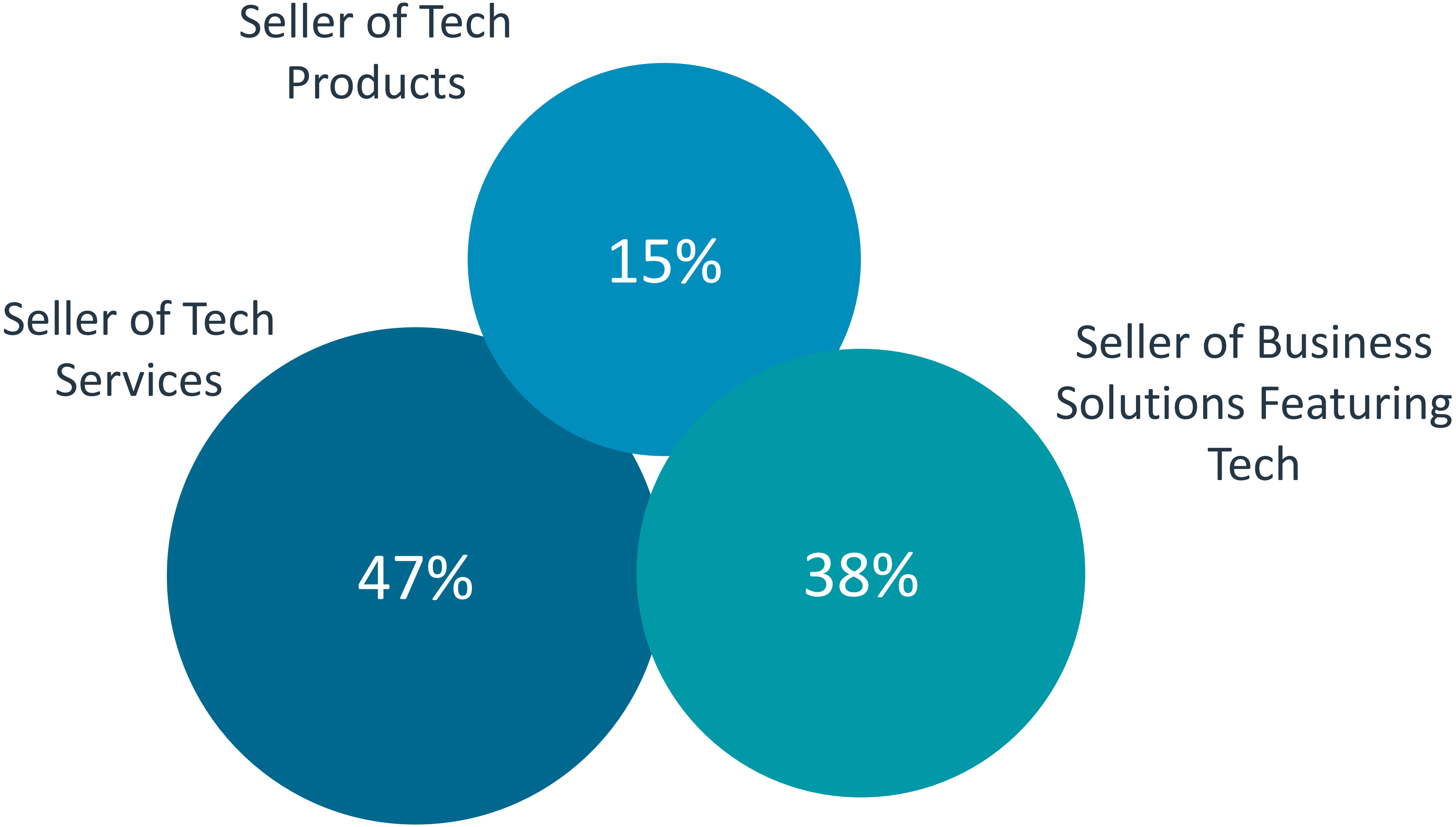
Top Priorities in Maintaining a Relevant and Future-Oriented IT Channel

	Australia & New Zealand	Benelux	ASEAN	UK & Ireland	DACH	North America
Top Positive Opportunity	Availability of generative AI tools & solutions	Availability of generative AI tools & solutions	Availability of generative AI tools & solutions	Technology's growing complexity creates demand for expertise	Technology's growing complexity creates demand for expertise	Technology's growing complexity creates demand for expertise
Top Negative Development	External factors (i.e., global economy, inflation, interest rates)	External factors (i.e., global economy, inflation, interest rates)	Competition from online marketplaces & non-traditional players (i.e. prof services firms)	Competition from online marketplaces & non-traditional players (i.e. prof services firms)	External factors (i.e., global economy, inflation, interest rates)	External factors (i.e., global economy, inflation, interest rates)

Channel practitioners will fill their to-do list with items ranging from how to embrace new technologies like AI; handle new types of competition and market changes; capitalize on new and more sophisticated services opportunities; optimize and improve internal business functions and better serve customers and the workforce.

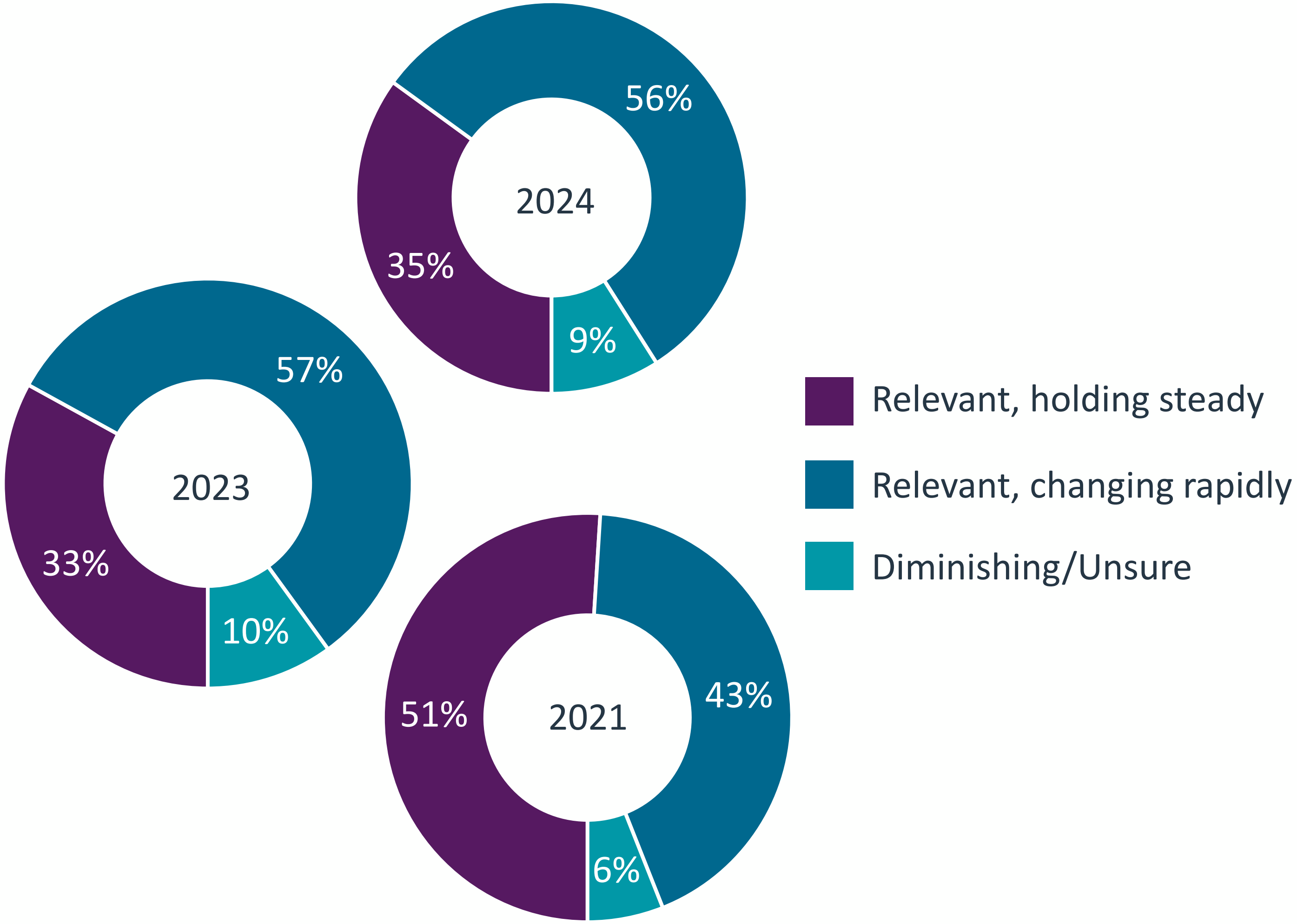
Source: CompTIA 2024 State of the Channel survey | n=1042 international respondents

How Channel Firms Describe Their Primary Business



Source: CompTIA 2024 State of the Channel survey | n=132 ANZ respondents

State of the IT Channel

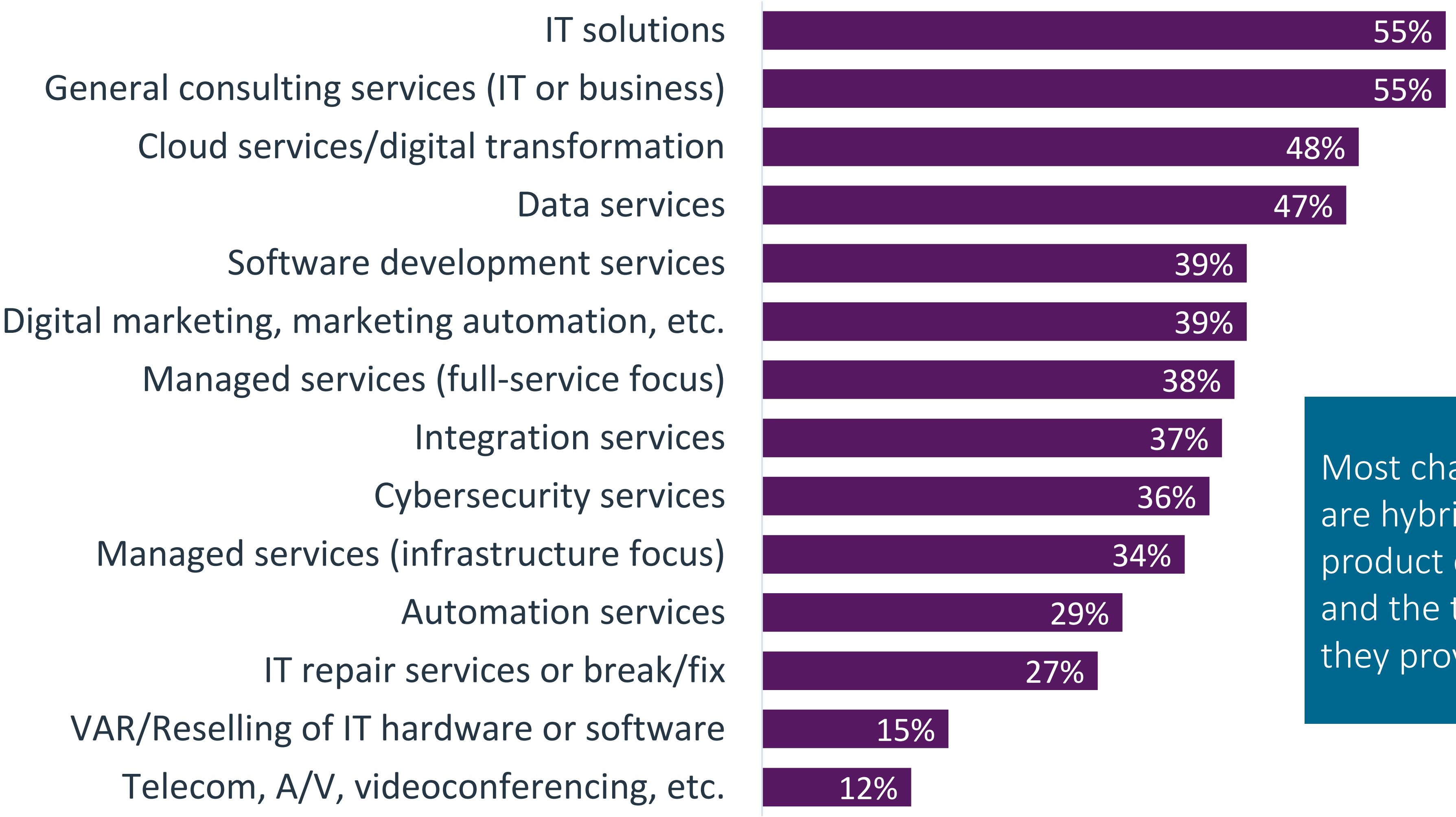


Factors Contributing to Healthy IT Channel

61%	Complexity of tech creating demand
58%	Adoption of generative AI tools
57%	Demand for cybersecurity services
47%	Adoption of cloud computing
40%	Demand for managed services
35%	Expanding channel business models

Source: CompTIA 2024 State of the Channel survey | 2024: n=132 ANZ respondents
2023: n=125 ANZ respondents
2021: n=125 ANZ respondents

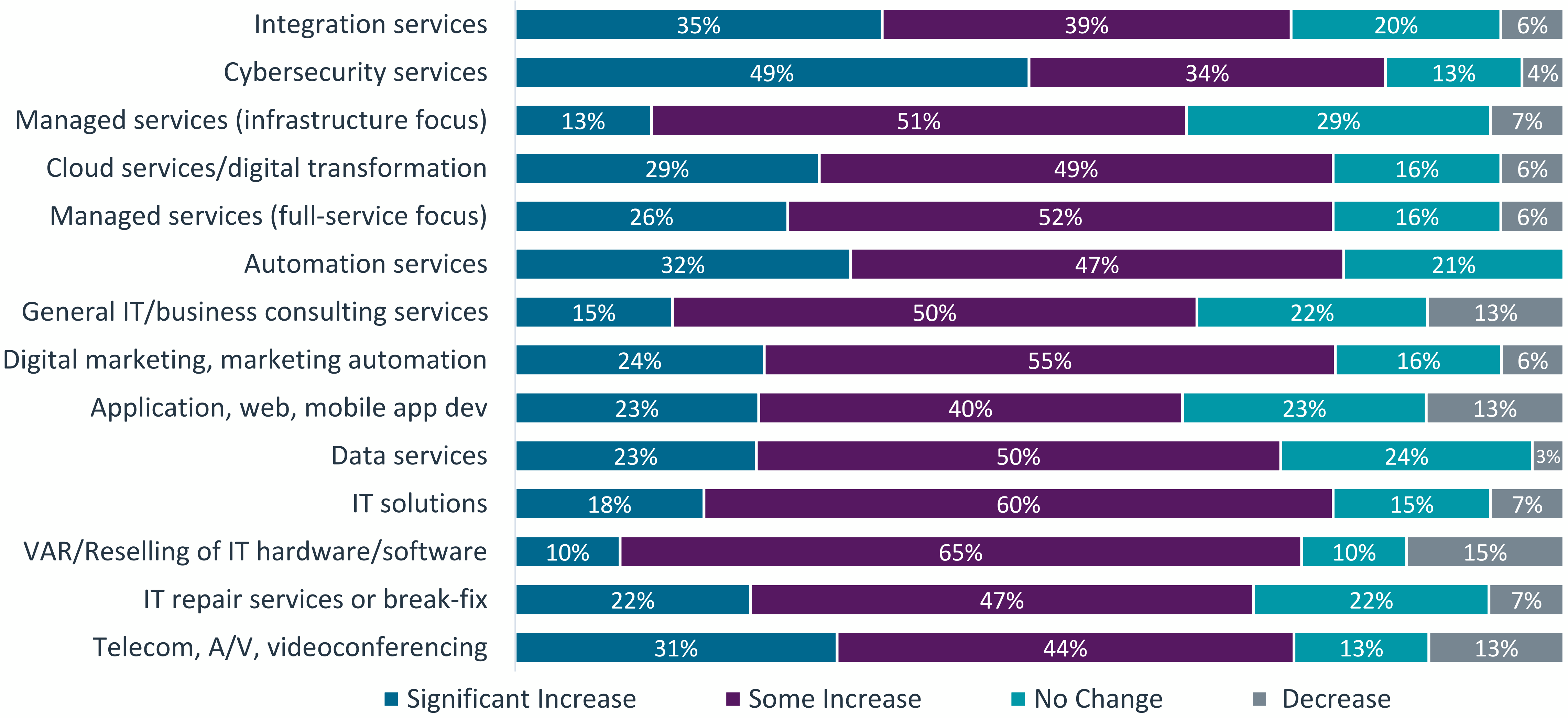
Company Lines of Business Offered



Most channel firms today are hybrid in terms of their product category offerings and the types of services they provide to customers.

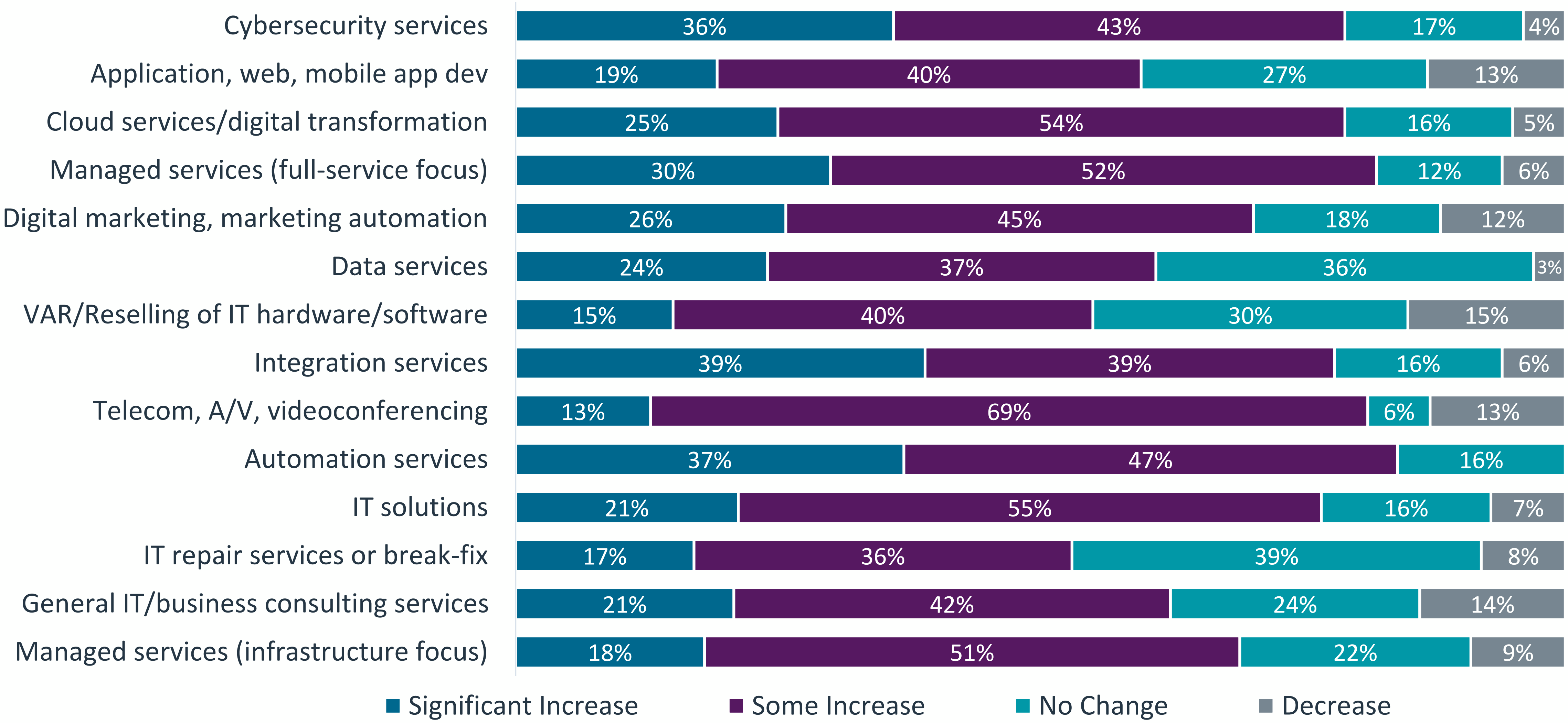
Source: CompTIA 2024 State of the Channel survey | n=132 ANZ respondents

Revenue Growth Expected Over Next Two Years



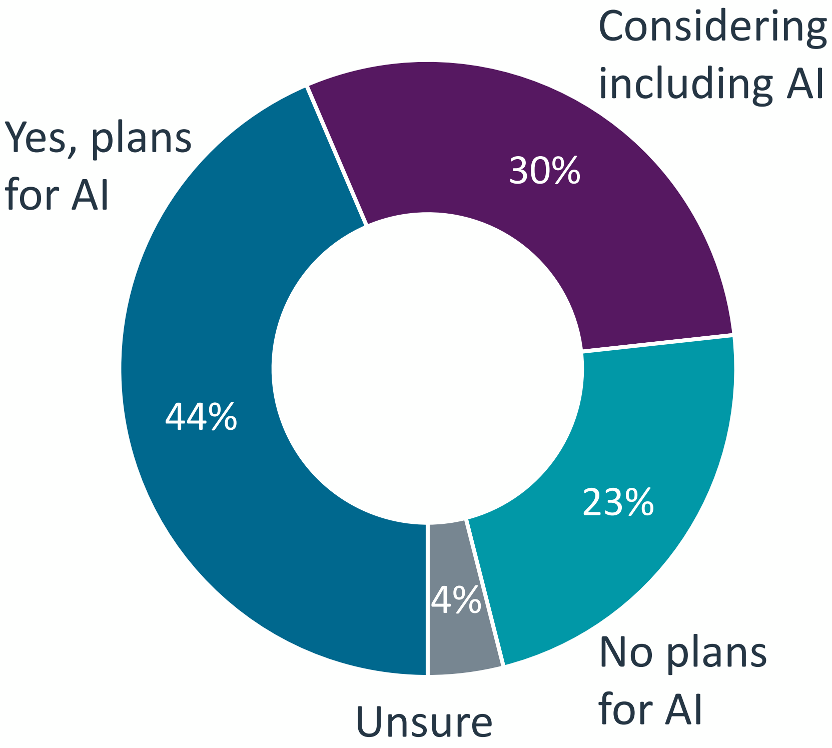
Source: CompTIA 2024 State of the Channel survey | n=132 ANZ respondents

Profit Margins Expected Over Next Two Years



Source: CompTIA 2024 State of the Channel survey | n=132 ANZ respondents

AI Solutions and Sales Over the Next Year



Customer experience

Sales and marketing

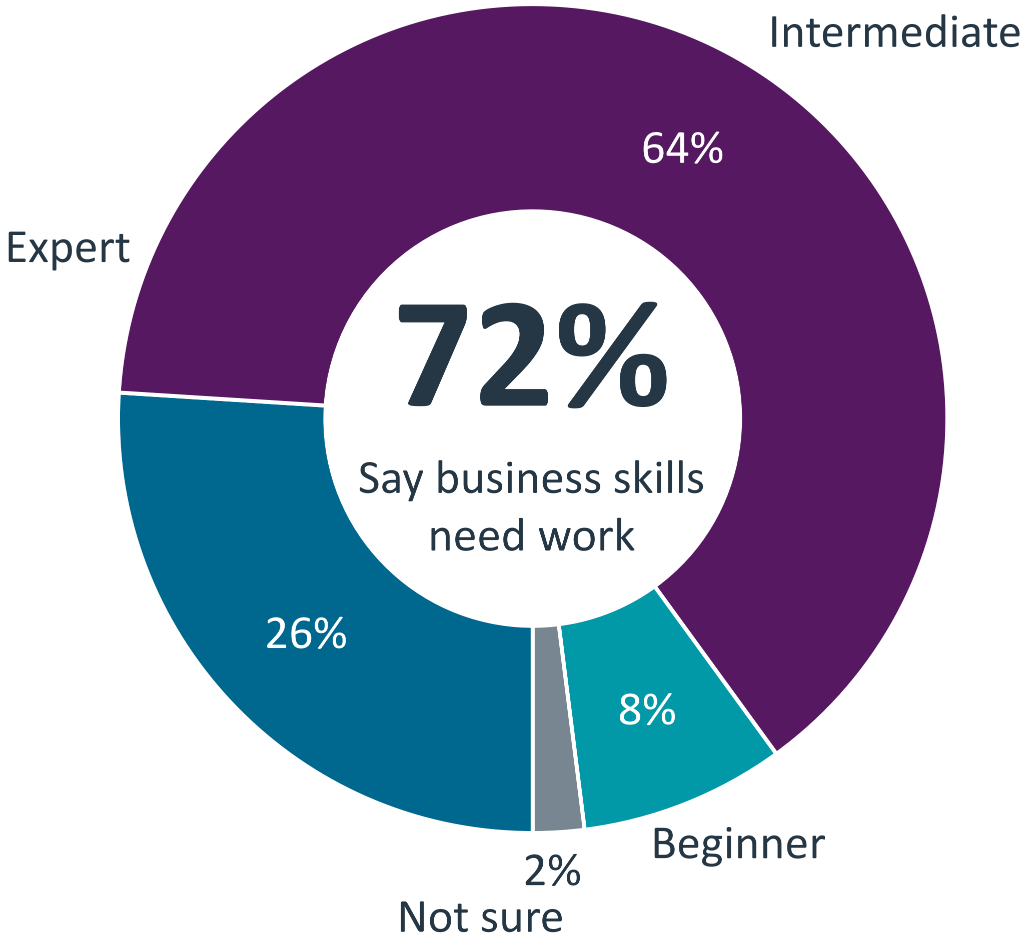
Operations

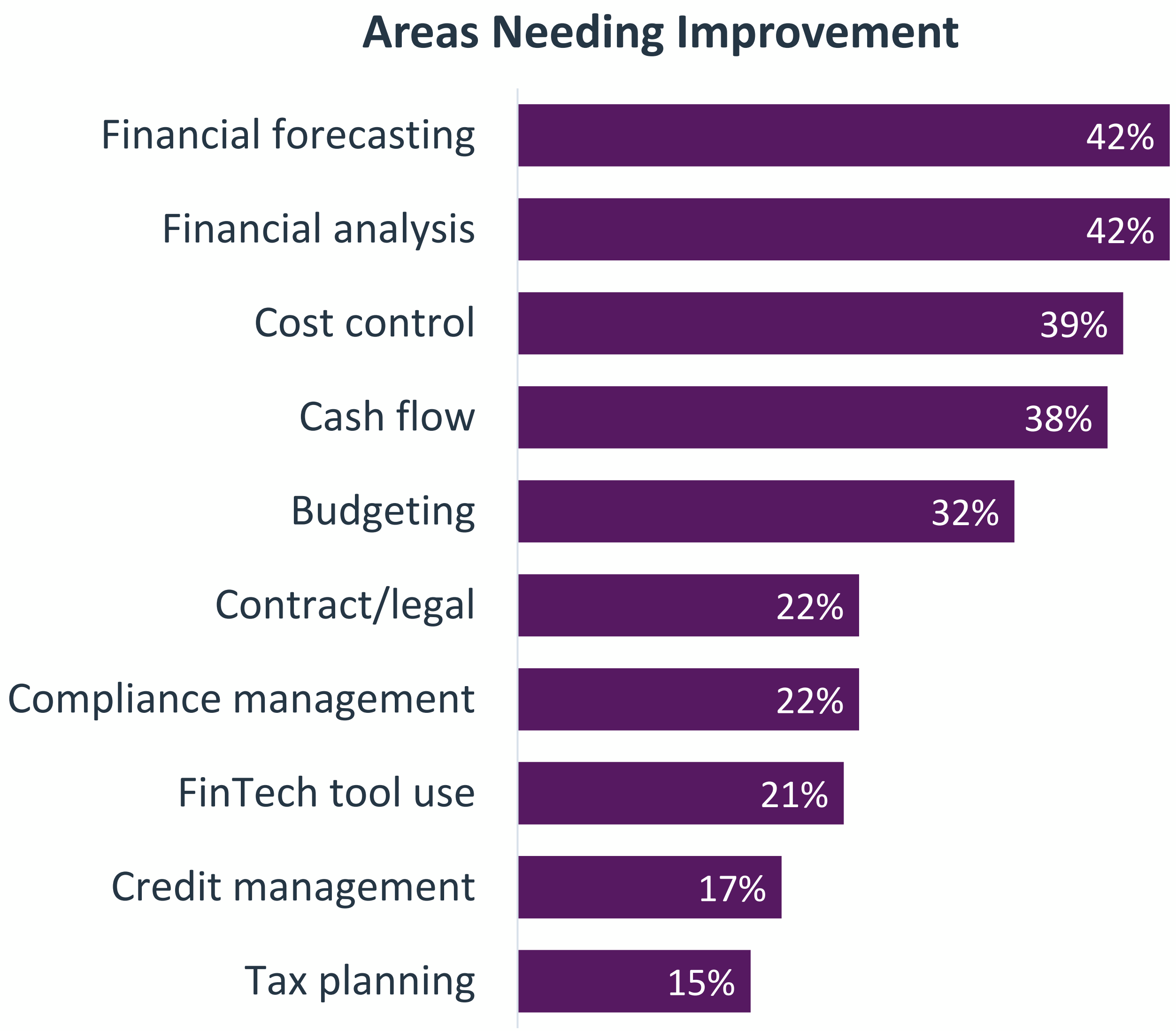
Business decision-making

Business management

Source: CompTIA 2024 State of the Channel survey | n=132 ANZ respondents

Self-Rating of Company's Business Acumen

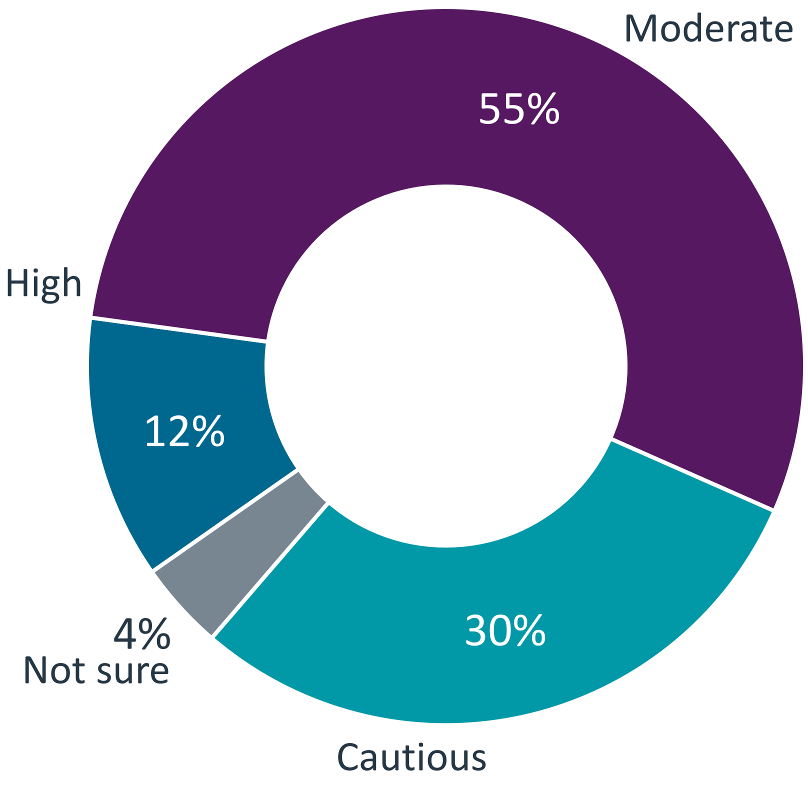




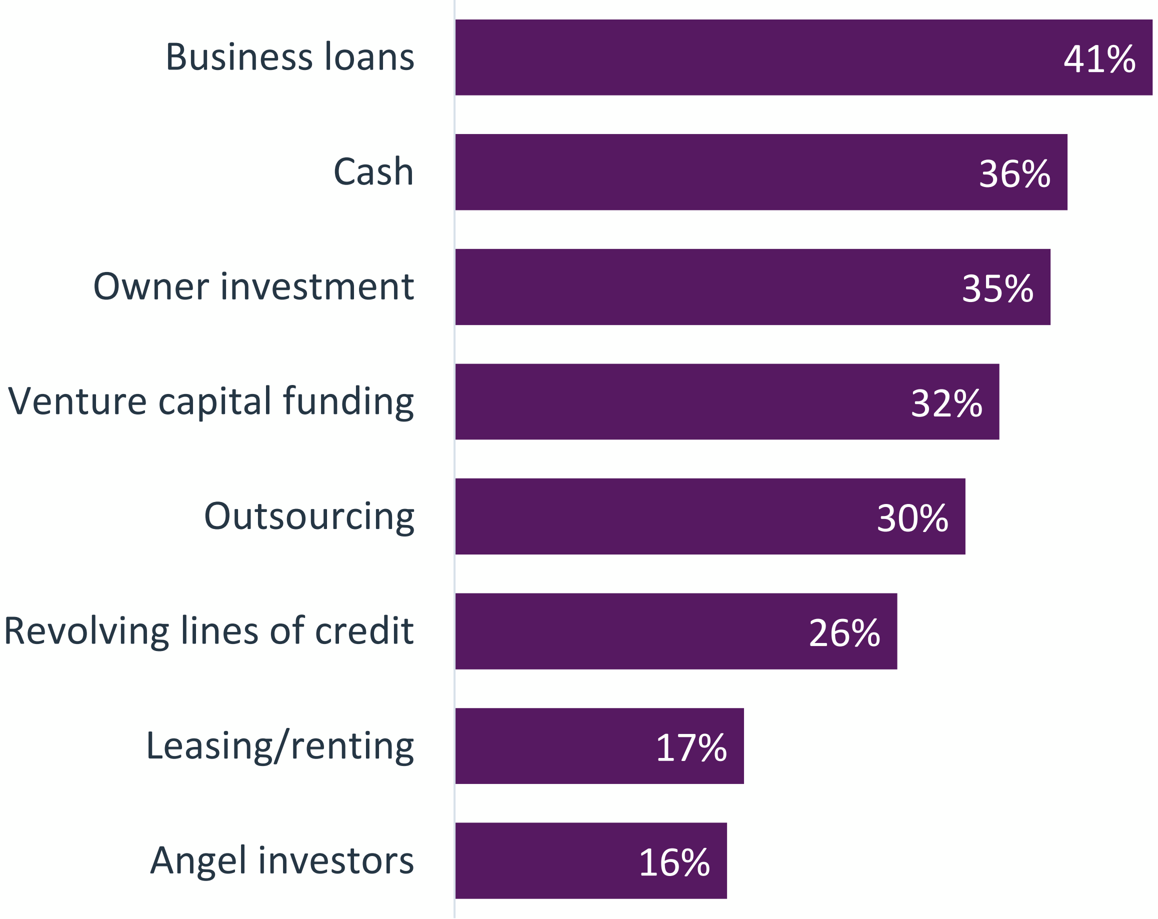
Source: CompTIA 2024 State of the Channel survey | n=132 ANZ respondents
96 ANZ respondents citing need for business acumen improvement

Operational Improvement Tied to Risk and Funding

Level of Financial Risk Tolerance

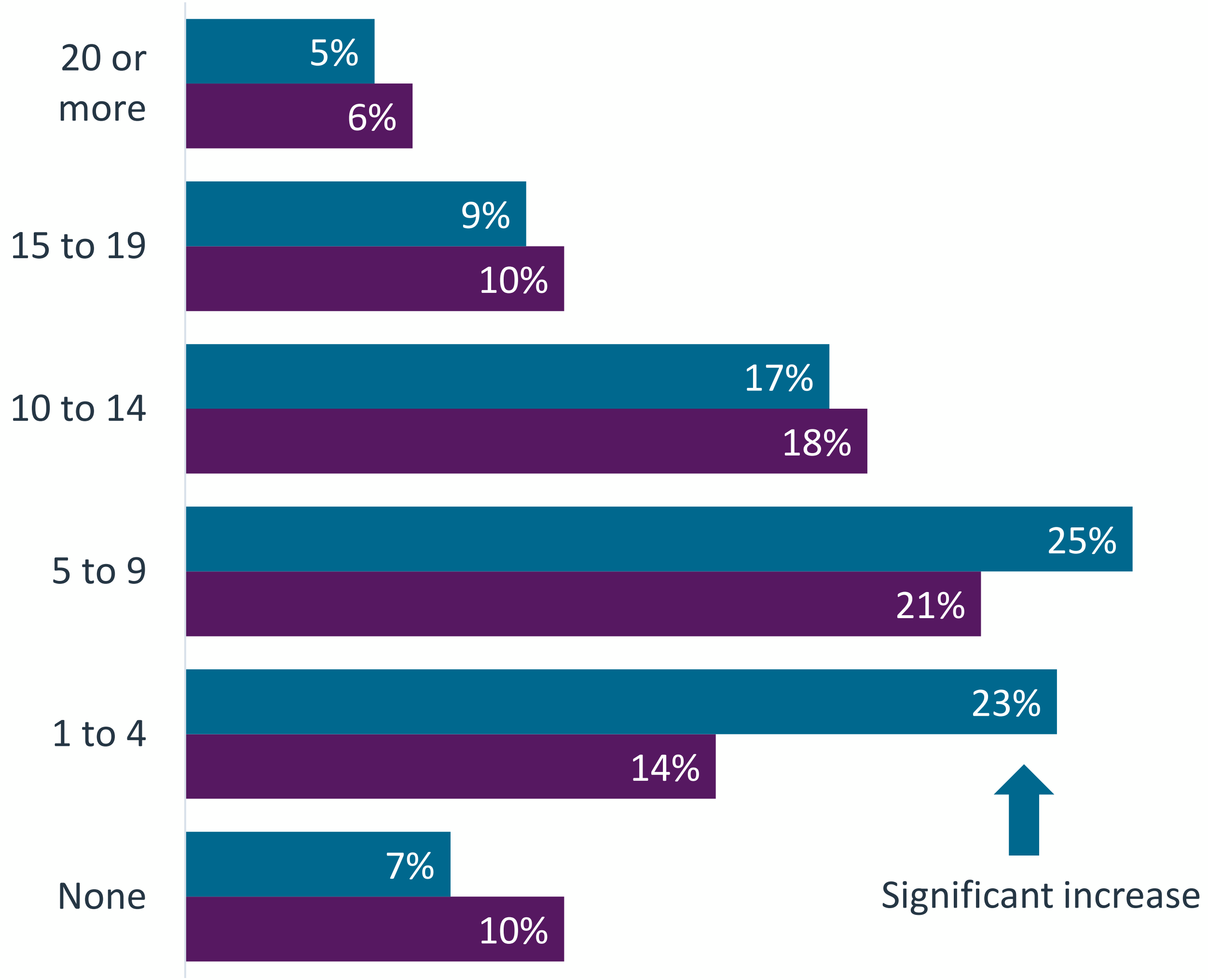


Sources of Funding Used by Companies



Source: CompTIA 2024 State of the Channel survey | n=132 ANZ respondents

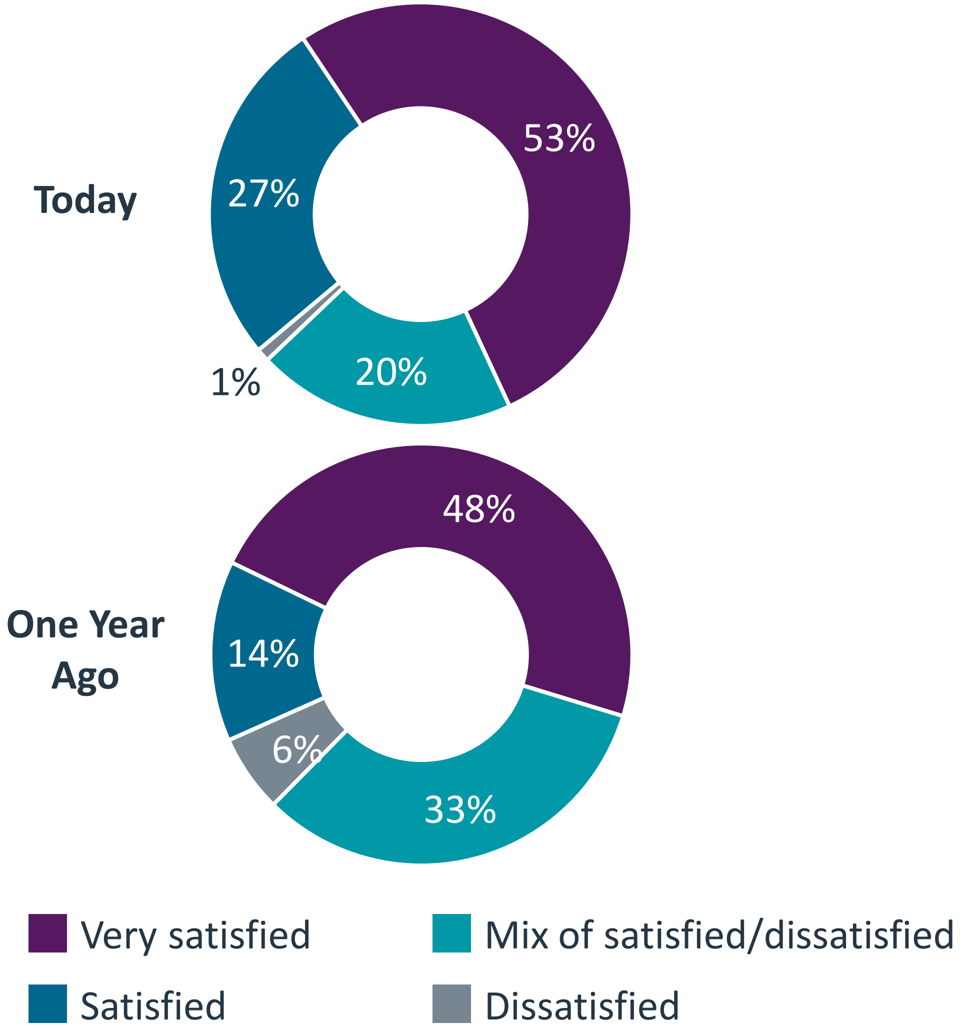
Number of Vendor Channel Partnerships



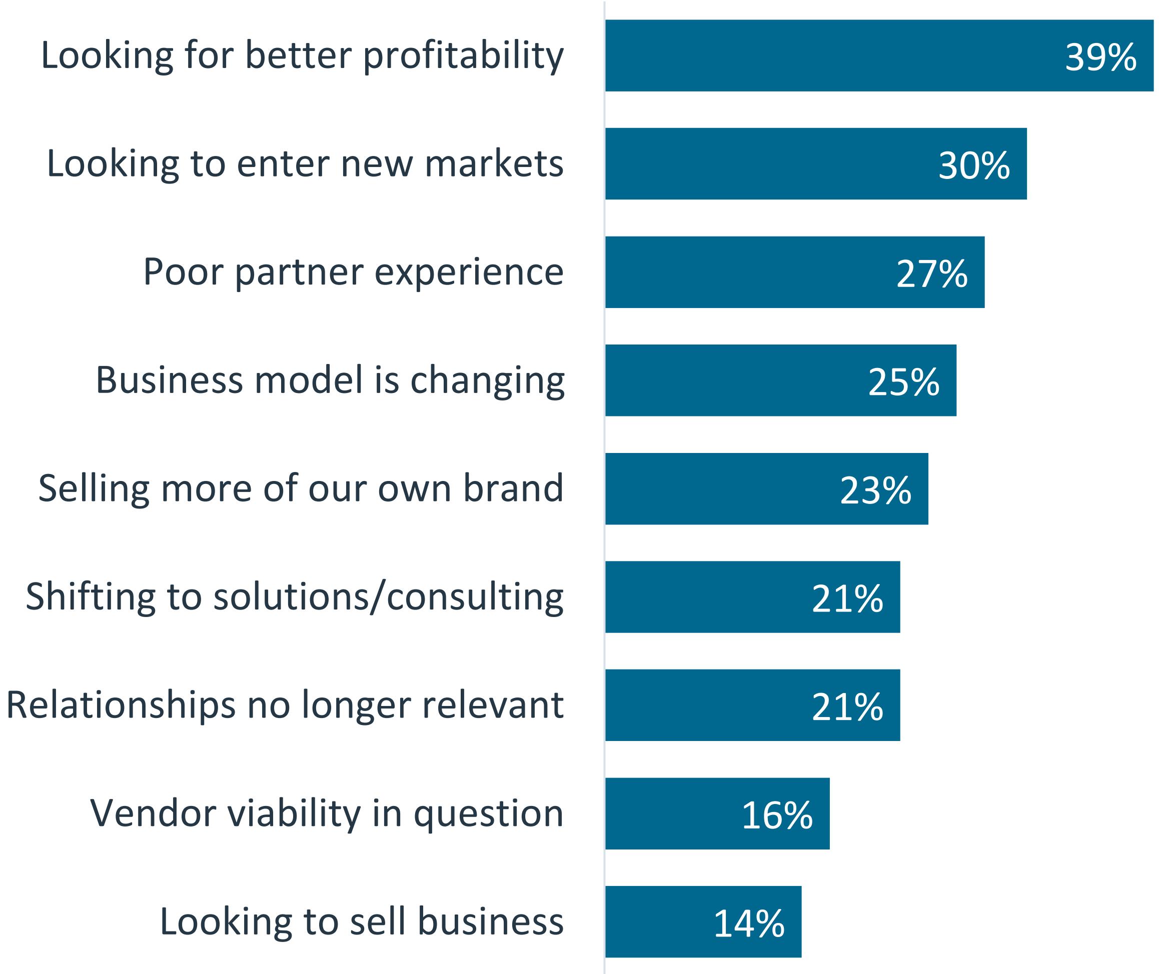
CompTIA

Source: CompTIA 2024 State of the Channel survey | 2024: n=132 ANZ respondents
2023: n=125 ANZ respondents

Channel Satisfaction Level With Vendors

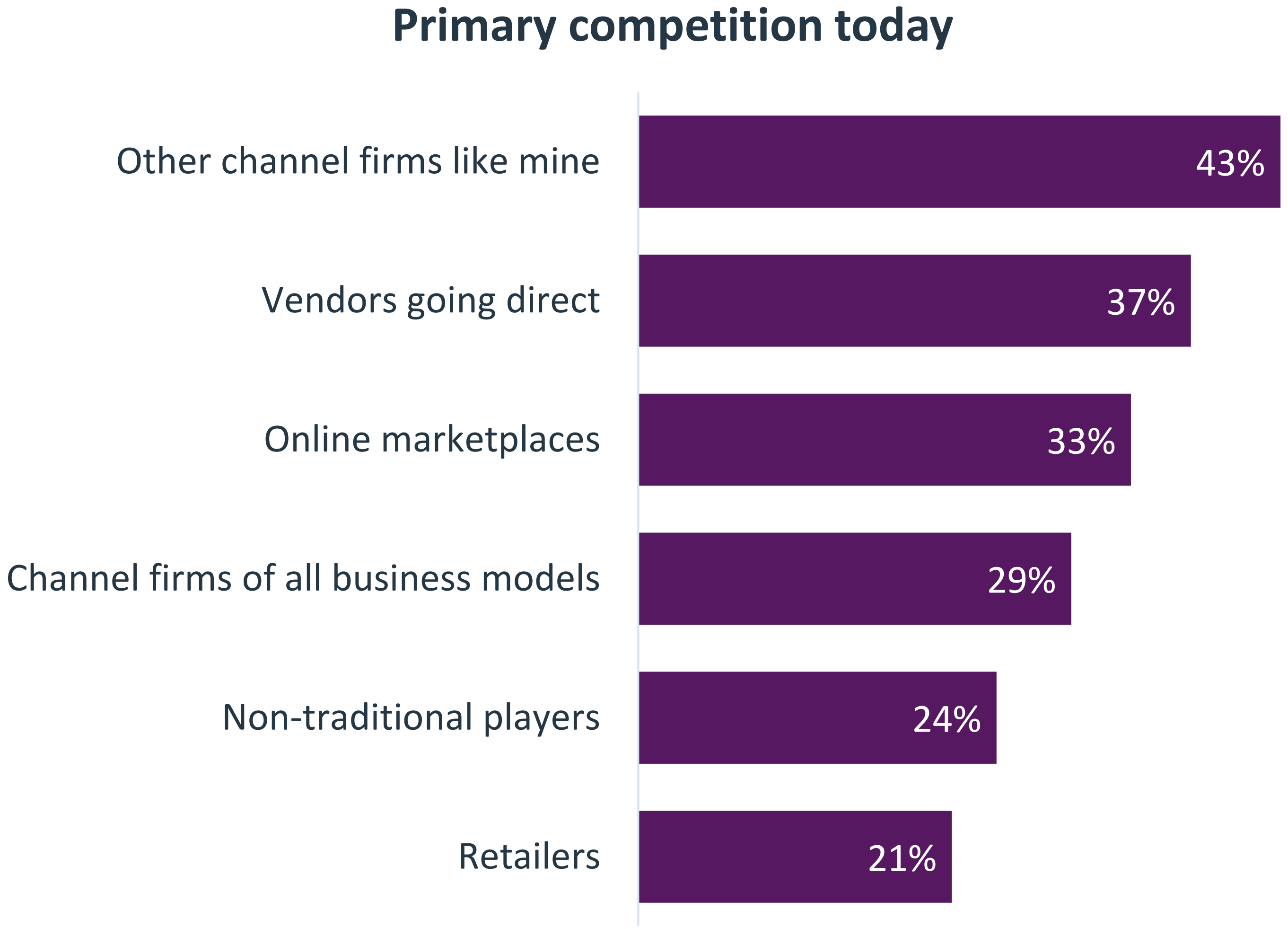


Reasons for Changes to Vendor Relationships



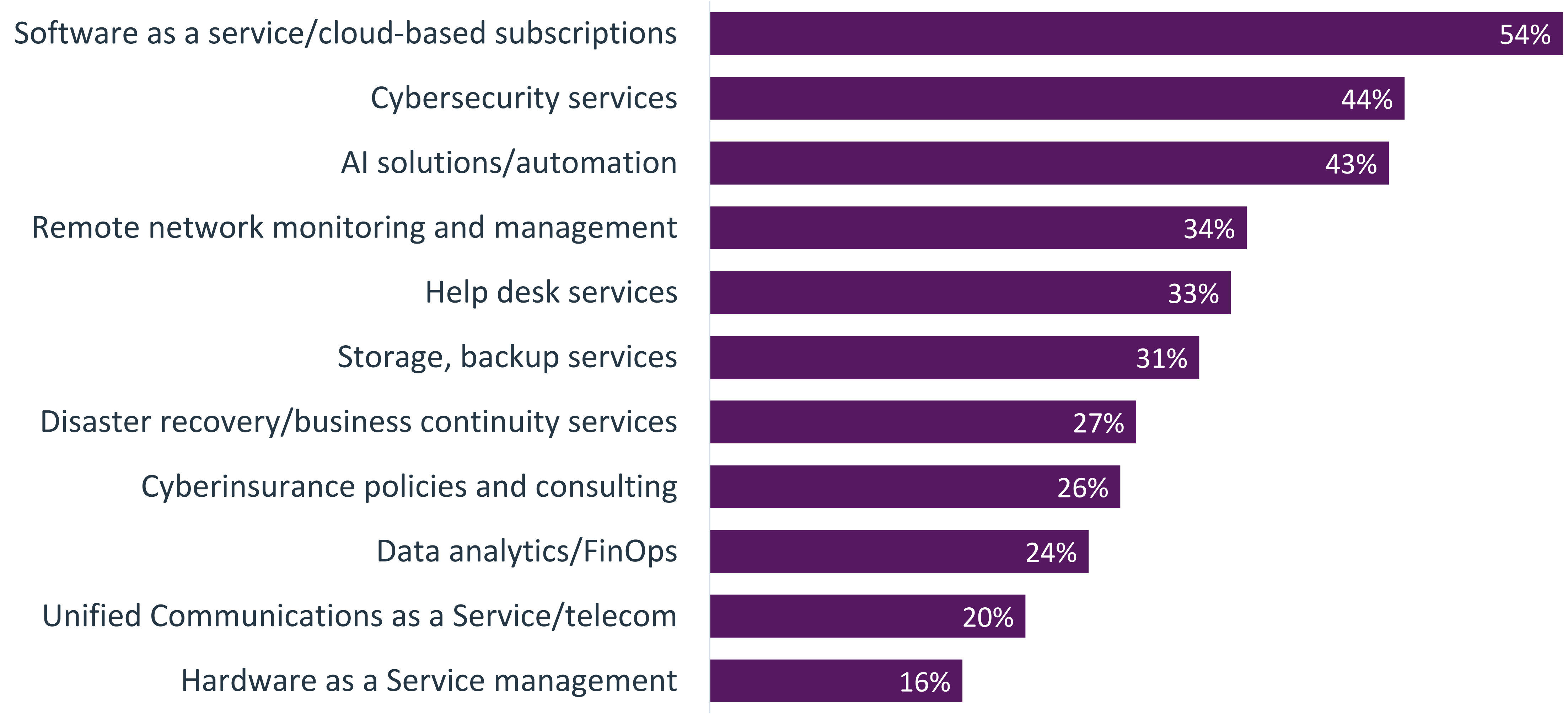
Source: CompTIA 2024 State of the Channel survey | n=132 ANZ respondents

View of Competitors in Business Today



Source: CompTIA 2024 State of the Channel survey | n=132 ANZ respondents

Most Requested MSP Services



Source: CompTIA 2024 State of the Channel survey | n=70 ANZ respondents offering managed services

Key Takeaways

- Services is the largest growing category in IT Spend
- Know what your customers want to buy
- Educate yourself & your staff to improve your business

Source: CompTIA 2024 State of the Channel survey | n=132 ANZ respondents

Adelaide Agenda

CompTIA Community

TIME	TOPIC
09:15 – 09:45 AM	**Welcome & Introduction** MJ Shoer, Chief Community Officer, CompTIA
09:45 – 10:00 AM	**Privacy Act Changes Impacting Your Business** David Norris, Managing Director, Nortec IT, Dean Calvert, Founder, Calvert Technologies
10:00 – 10:30 AM	**State of Cybersecurity.** David Norris, Managing Director, Nortec IT
10:30 – 11:00 AM	**MORNING TEA & NETWORKING BREAK**
11:00 – 11:30 AM	**Securing Active Directory:** KRBTGT Resets After Credential Theft. Samuel Freeman, Senior Investigator DFIR, CyberCX
11:30 AM – 12:30 PM	**Risk Management for your business. Part 1.** Wayne Selk, VP Cybersecurity Programs, CompTIA
12:30 – 12:35 PM	**QUICK BREAK**
12:35 – 1:00 PM	**State of the Channel, with ANZ Perspectives.** Maria Armstrong, Manager of Academy APAC, Pax8
1:00 – 2:00 PM	**LUNCH & NETWORKING**

WE ARE THE CompTIA® Community

1:00 – 2:00 PM

LUNCH & NETWORKING

Adelaide Agenda

CompTIA Community

TIME	TOPIC
2:00 – 2:20 PM	**A comedy spot** after lunch with Rob Farley.
2:25 – 3:05 PM	Why Your Customers Need Cybersecurity Insurance. Andrew Bremner, SherpaTech
3:05 – 3:10 PM	**QUICK BREAK**
3:10 – 4:00 PM	**Risk Management for your business. Part 2.** Wayne Selk, VP, Cybersecurity Programs, CompTIA
4:00 – 4:05 PM	**QUICK BREAK**
4:00 – 4:30 PM	**Fireside Chat** MJ Shoer & Wayne Selk – CompTIA
4:30 – 5:00 PM	**NETWORKING DRINKS & CANAPES**

WE ARE THE CompTIA® Community

A COMEDY SPOT

Rob Farley, Owner/Principal, Lobster Pot Solutions

Adelaide Agenda

CompTIA Community

TIME	TOPIC
2:00 – 2:20 PM	**A comedy spot** after lunch with Rob Farley.
2:25 – 3:05 PM	**Why Your Customers Need Cybersecurity Insurance**. Andrew Bremner, SherpaTech
3:05 – 3:10 PM	**QUICK BREAK**
3:10 – 4:00 PM	**Risk Management for your business. Part 2.** Wayne Selk, VP, Cybersecurity Programs, CompTIA
4:00 – 4:05 PM	**QUICK BREAK**
4:00 – 4:30 PM	**Fireside Chat** MJ Shoer & Wayne Selk – CompTIA
4:30 – 5:00 PM	**NETWORKING DRINKS & CANAPES**

WE ARE THE CompTIA® Community

WHY YOUR CUSTOMERS NEED CYBERSECURITY INSURANCE

Andrew Bremner, MD, Sherpatech Insurance

Adelaide Agenda

CompTIA Community

TIME	TOPIC
2:00 – 2:20 PM	**A comedy spot** after lunch with Rob Farley.
2:25 – 3:05 PM	**Why Your Customers Need Cybersecurity Insurance.** Andrew Bremner, SherpaTech
3:05 – 3:10 PM	**QUICK BREAK**
3:10 – 4:00 PM	**Risk Management for your business. Part 2.** Wayne Selk, VP, Cybersecurity Programs, CompTIA
4:00 – 4:05 PM	**QUICK BREAK**
4:00 – 4:30 PM	**Fireside Chat** MJ Shoer & Wayne Selk – CompTIA
4:30 – 5:00 PM	**NETWORKING DRINKS & CANAPES**

WE ARE THE CompTIA® Community

3:05 – 3:10 PM

QUICK BREAK

Adelaide Agenda

TIME	TOPIC
2:00 – 2:20 PM	**A comedy spot** after lunch with Rob Farley.
2:25 – 3:05 PM	**Why Your Customers Need Cybersecurity Insurance.** Andrew Bremner, SherpaTech
3:05 – 3:10 PM	**QUICK BREAK**
3:10 – 4:00 PM	**Risk Management for your business. Part 2.** Wayne Selk, VP, Cybersecurity Programs, CompTIA
4:00 – 4:05 PM	**QUICK BREAK**
4:00 – 4:30 PM	**Fireside Chat** MJ Shoer & Wayne Selk – CompTIA
4:30 – 5:00 PM	**NETWORKING DRINKS & CANAPES**

WE ARE THE CompTIA® Community

3:10 – 4:00 PM

RISK MANAGEMENT FOR YOUR BUSINESS. PART 2

WAYNE SELK, VP, CYBERSECURITY PROGRAMS, COMPTIA

Operationalizing Risk within the Organization

Part 2

CompTIA CYBERSECURITY Programs

What is this Course?

Cybersecurity Trustmark Risk Management Course

- This course is an immersive dive into the world of business risk
- Each Part is approximately ONE Hour
- In the five-part series, you will learn to:
  - Understand Business Risk – Part 1
  - Operationalize Your Risk – Part 2
  - Help Your Clients Understand Their Risk – Part 3
  - Create a Strategy for Risk – Part 4
  - Create Opportunity for Risk – Part 5

What Will I Be Learning Today

Agenda

- Business Risk - Defined
- Seven Types of Business Risk
- Assumptions
- Uncovering Risk
- The “Methodology”
- Ensuring Proper Alignment
- Getting Ready to Help Your Clients with Their Risk

Business Risk - Defined

Important

The Hartford defines business risk as:

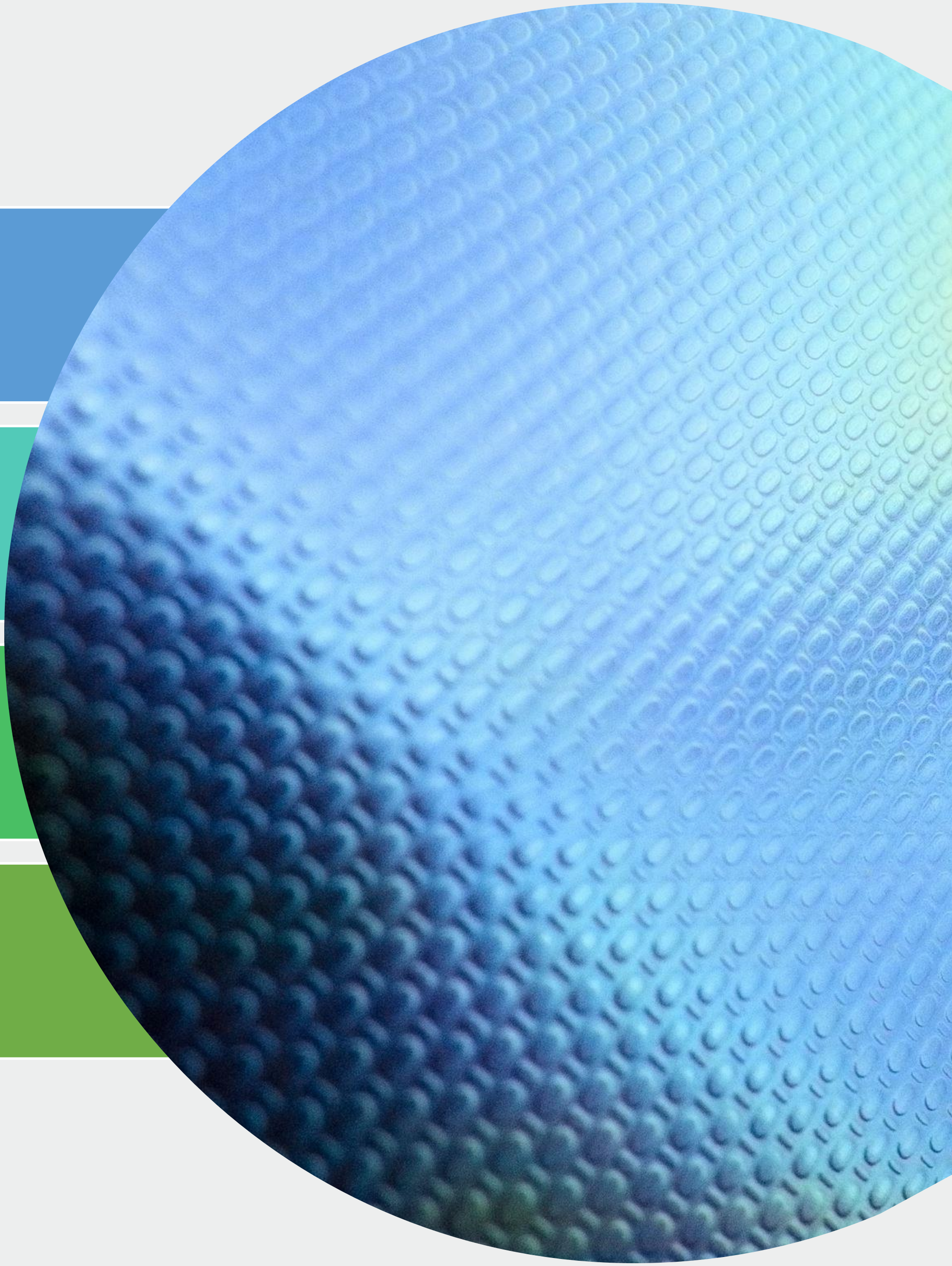
“anything that could impact your company’s finances”

7 Types of Business Risk

- Strategic
- Compliance
- Financial
- Operational
- Reputational
- Global
- Competitive

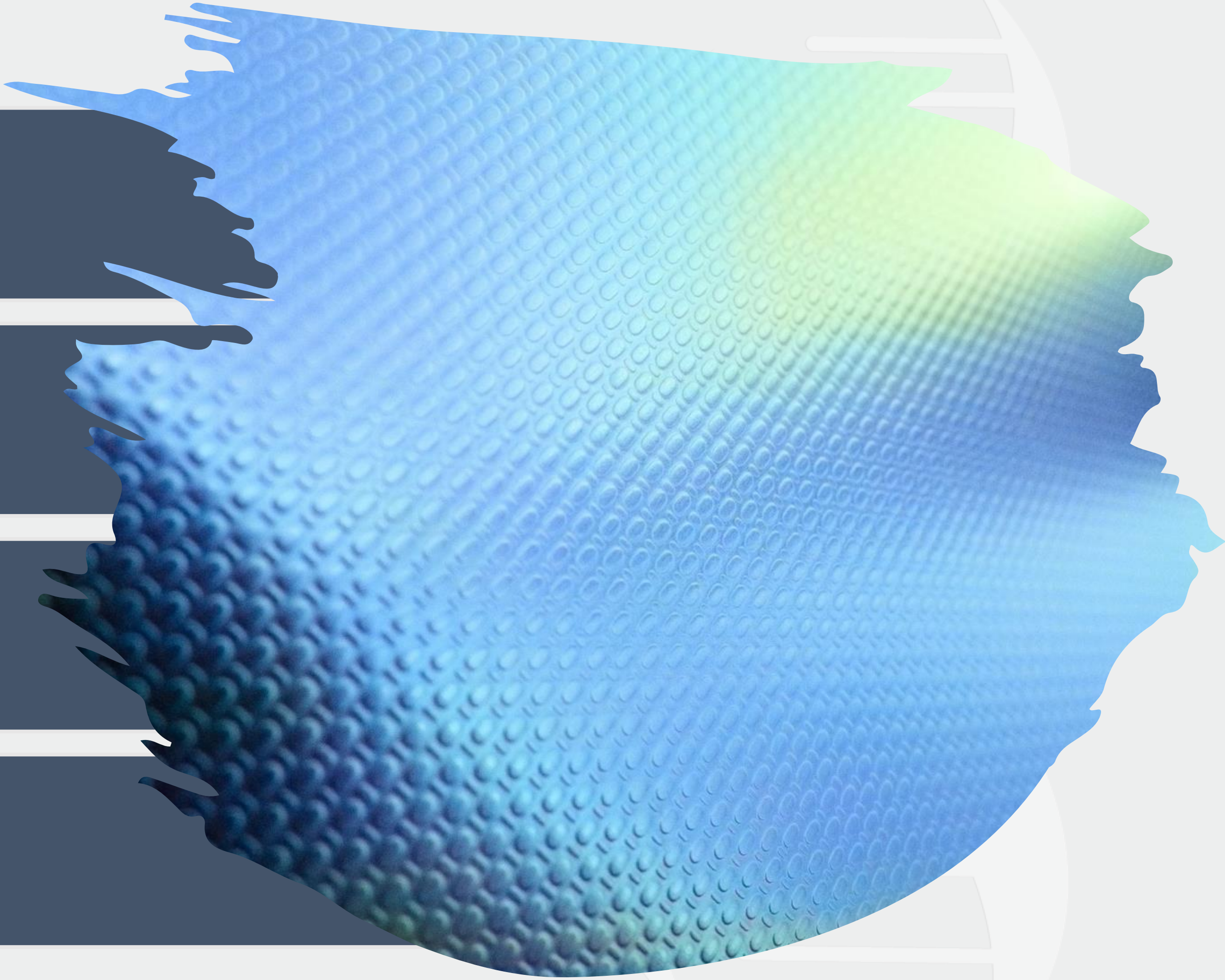
Strategic Risk

- Technology Changes
- Competitive Pressure
- Legal Changes
- Shifts in Customer Demand



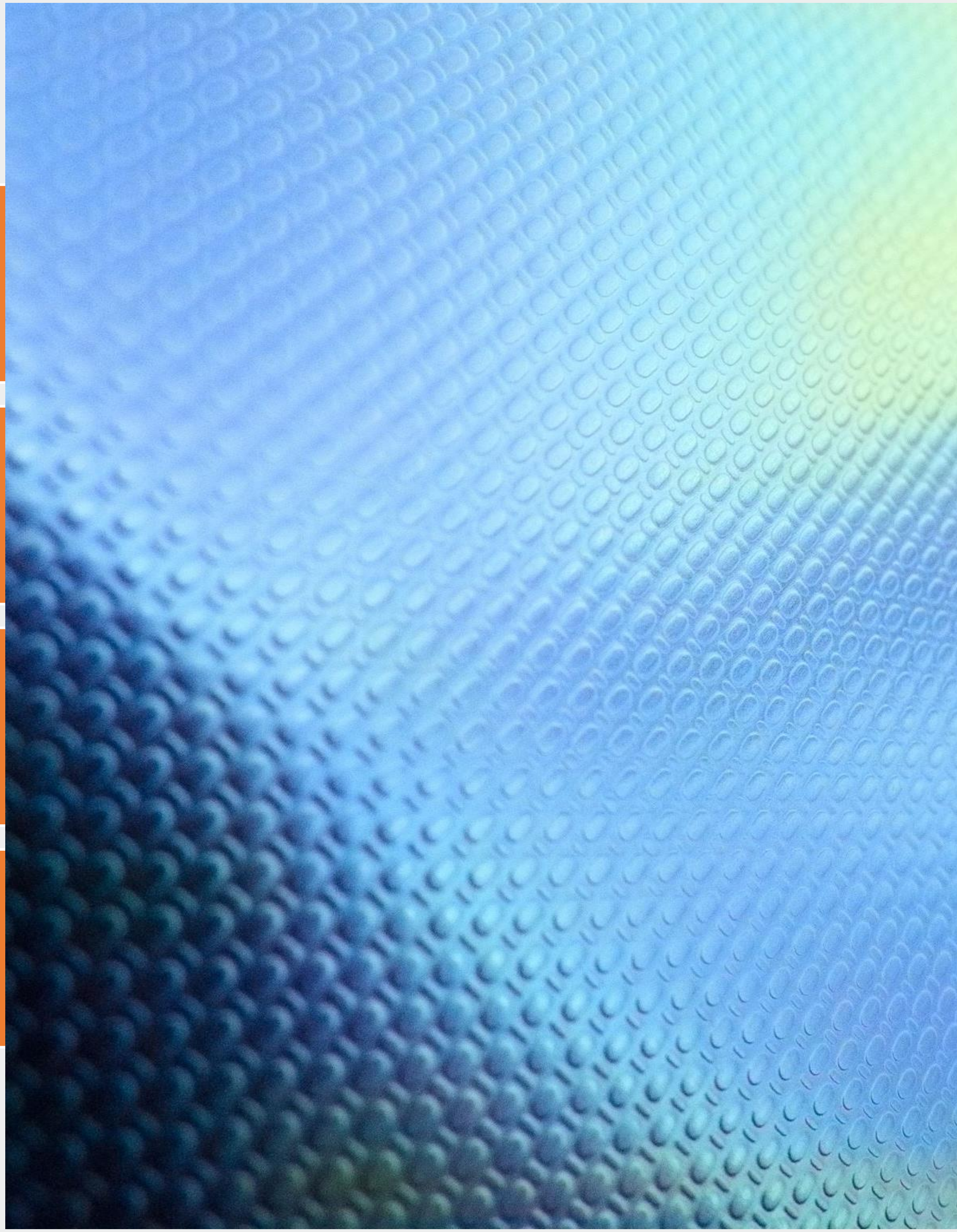
Compliance Risk

- Insider Threats
- Data Storage Issues
- Data Availability
- Data Theft



Financial Risk

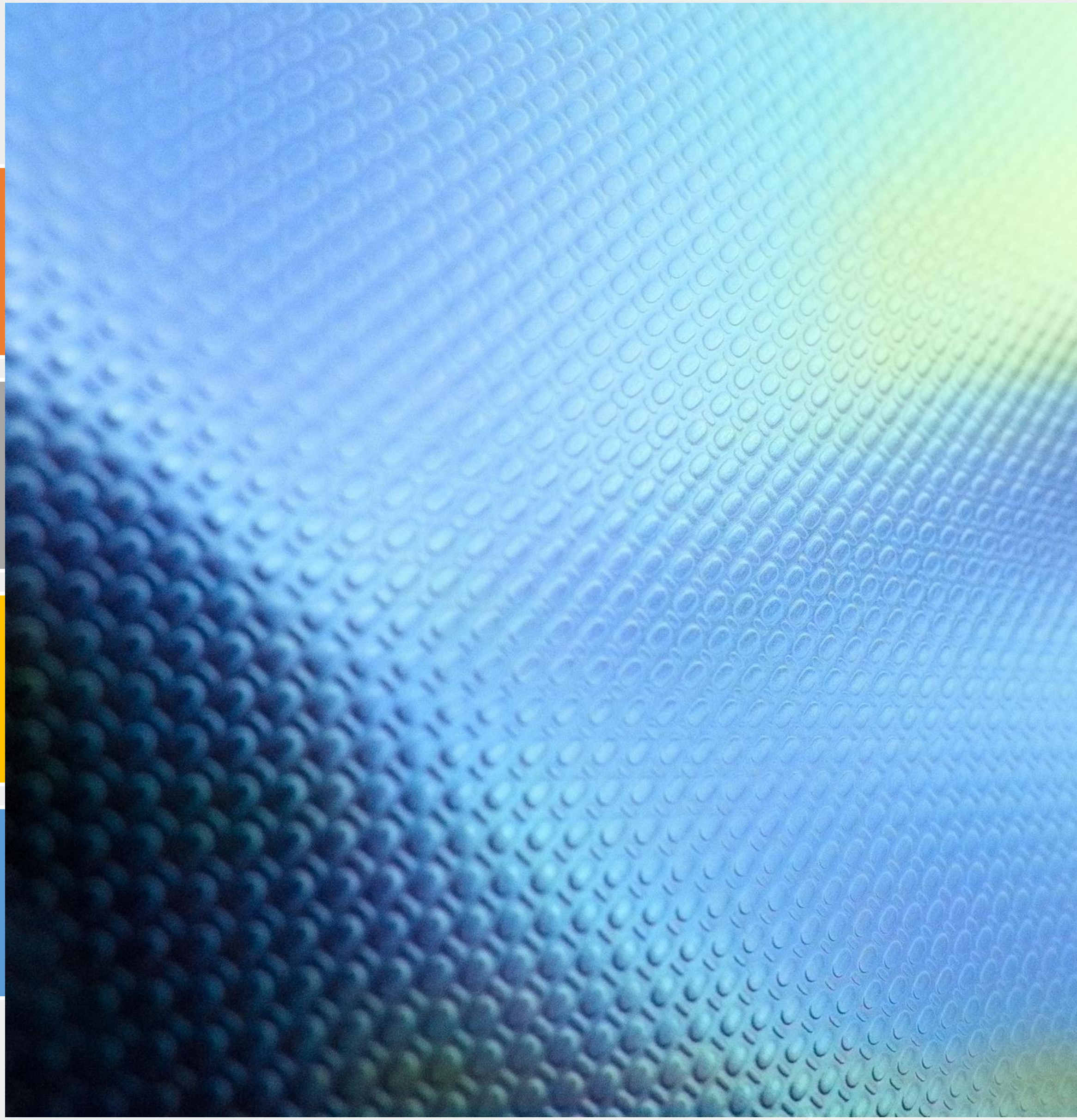
- Cash Flow
- Economic Changes
- Debt to Profit Ratio
- Loss of Customers



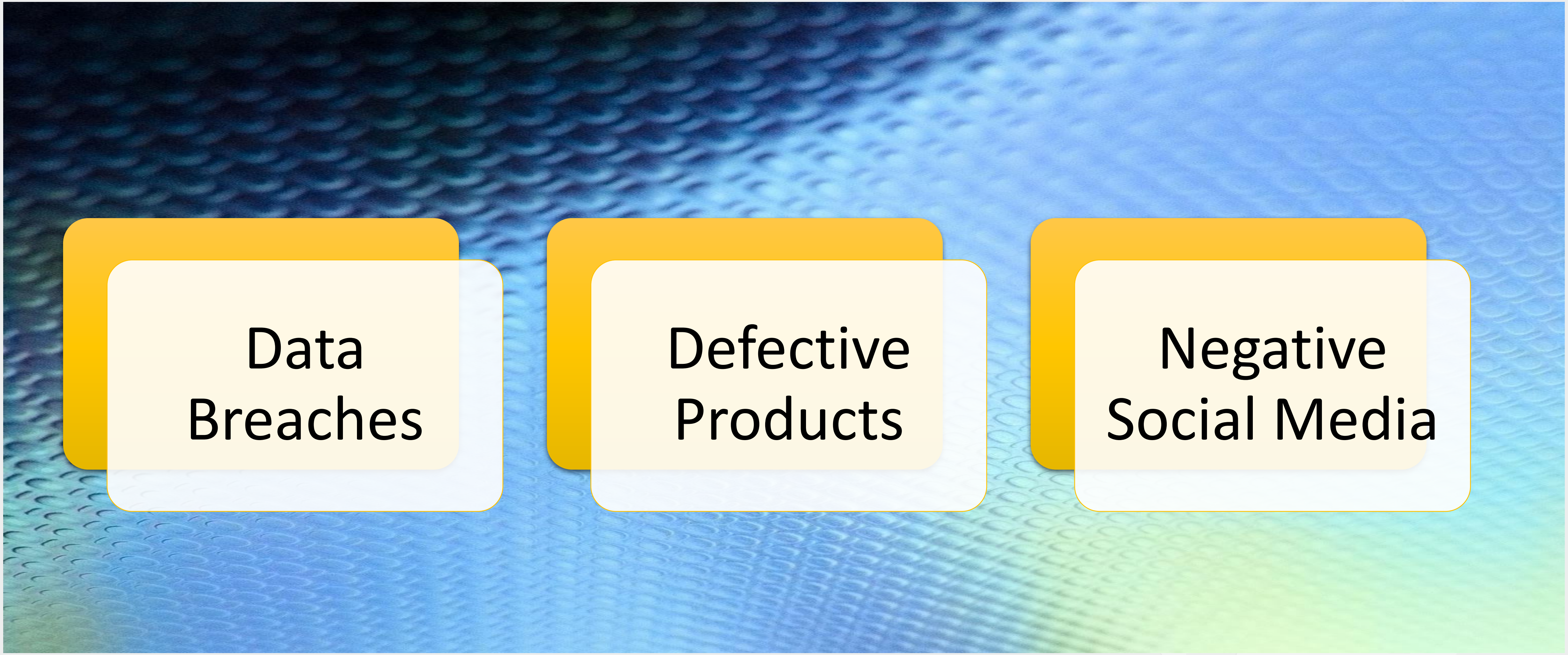
CompTIA CYBERSECURITY Programs

Operational Risk

- Natural Disasters
- Theft
- Failures in Technology
- Changes in Laws



Reputational Risk



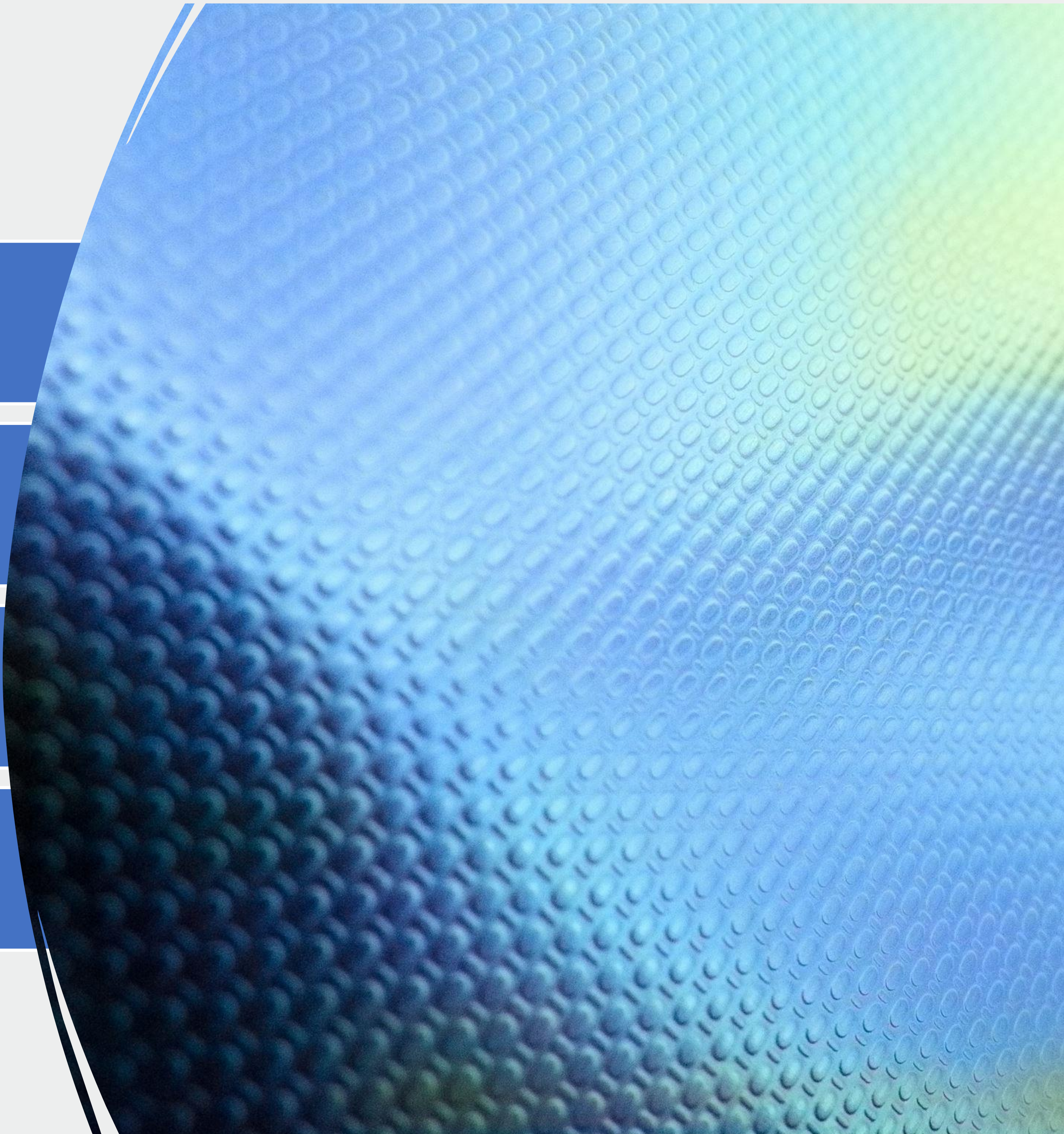
Data Breaches

Defective Products

Negative Social Media

Global Risk

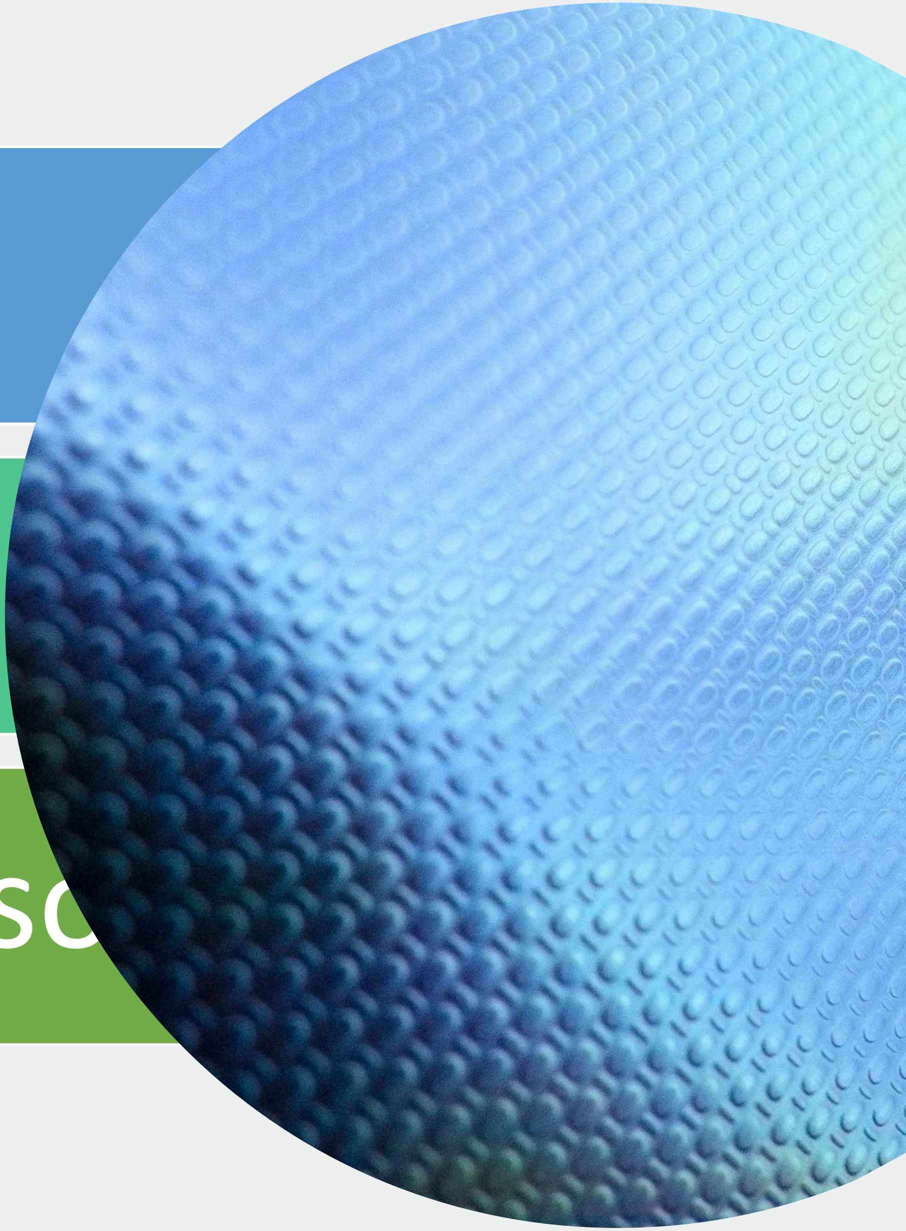
- Espionage
- War/Conflict
- Economic Stability
- Supply Disruption



CompTIA CYBERSECURITY Programs

Competitive Risk

- Marketing
- Better Services
- Loss of Experienced Perso



Assumptions or More Risk?

- “That is the way we have always done it”
- We have security controls
- “We are too small”
- Look only at the big items
- Others?

Uncovering Risk

- BREAK DOWN THE BIG PICTURE
- BE PESSIMISTIC
- CONSULT AN EXPERT
- SEEK EMPLOYEE FEEDBACK – REGULARLY
- ANALYZE CUSTOMER COMPLAINTS
- CONDUCT INTERNAL AND EXTERNAL RESEARCH

Homework Review

Did you do it?

- Did you identify your Business Objective?
- When looking at your risks, did you reflect internally first?
  - If not, what kind of risks did you potentially miss?
  - What impact would those risks have on your business?
- Did anyone find themselves losing focus on the business objective?
- Last question – How will the three areas impact your objective?
  - Please share your business objective, then discuss the impact(s)

Business Plan

Every business should have one…

- Roadmap to follow for business success
- 3-5, 7, 10 year plan
- Objectives and Milestones
- Risks to prevent achieving (when written)
- Exit Strategy

The "Methodology"

Business Objectives

Business Risks

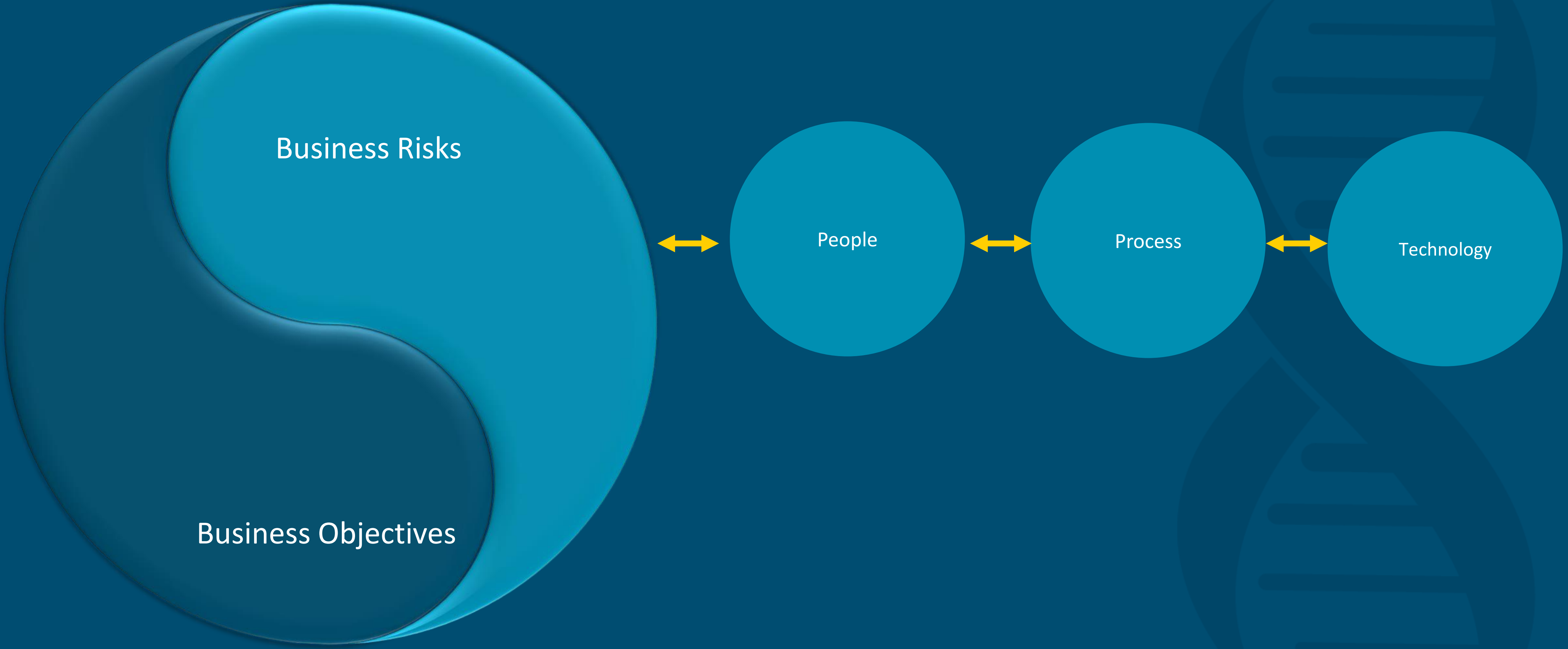
People

Process

Technology

Ensure Proper Alignment

Or risk failure



CompTIA CYBERSECURITY Programs

Helping your Clients

Yep, Part 3!

- Understand their Business Objectives (Build a solution for success)
- Is Compliance or Regulatory part of their business?
- Focus on Key Talking Points (HINT: Never discuss Technology/Never discuss FUD)
    1. Cost of an Incident or Compromise
    2. Nothing is 100% - it is about reducing IMPACT
    3. Employees make mistakes – when they do, remind of 1 & 2
    4. As the Data Owner they own the liability and budget
- Importance of Continuous Monitoring (HINT: Not everyone is ready for this)

Thank YOU!

CompTIA CYBERSECURITY Programs

Adelaide Agenda

TIME	TOPIC
2:00 – 2:20 PM	**A comedy spot** after lunch with Rob Farley.
2:25 – 3:05 PM	**Why Your Customers Need Cybersecurity Insurance.** Andrew Bremner, SherpaTech
3:05 – 3:10 PM	**QUICK BREAK**
3:10 – 4:00 PM	**Risk Management for your business. Part 2.** Wayne Selk, VP, Cybersecurity Programs, CompTIA
4:00 – 4:30 PM	**Fireside Chat** MJ Shoer & Wayne Selk – CompTIA
4:30 – 5:00 PM	**NETWORKING DRINKS & CANAPES**

WE ARE THE CompTIA® Community

4:00 – 4:05 PM

QUICK BREAK

Adelaide Agenda

CompTIA Community

TIME	TOPIC
2:00 – 2:20 PM	**A comedy spot** after lunch with Rob Farley.
2:25 – 3:05 PM	**Why Your Customers Need Cybersecurity Insurance.** Andrew Bremner, SherpaTech
3:05 – 3:10 PM	**QUICK BREAK**
3:10 – 4:00 PM	**Risk Management for your business. Part 2.** Wayne Selk, VP, Cybersecurity Programs, CompTIA
4:00 – 4:05 PM	**QUICK BREAK**
4:00 – 4:30 PM	**Fireside Chat** MJ Shoer & Wayne Selk – CompTIA
4:30 – 5:00 PM	**NETWORKING DRINKS & CANAPES**

WE ARE THE CompTIA® Community

Gerardo Barranquero, Aso

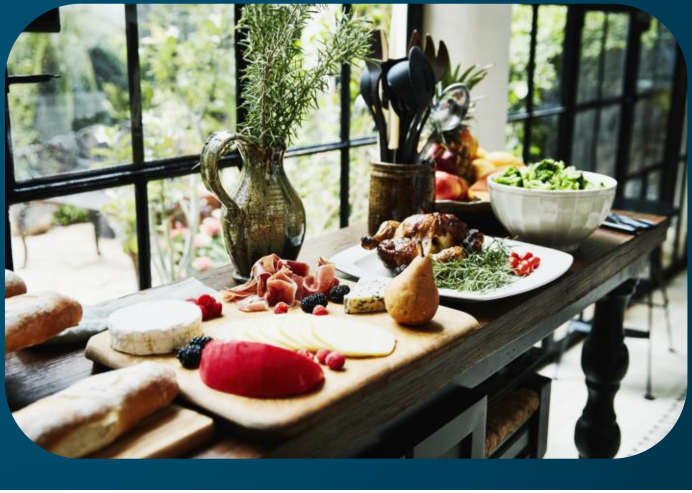
4:00 -4:30 pm

FIRESIDE CHAT WITH MJ AND WAYNE

MJ SHOER, CHIEF COMMUNITY OFFICER , COMPTIA

WAYNE SELK, VP CYBERSECURITY PROGRAMS, COMPTIA.

WE ARE THE CompTIA® Community



4:30 – 5:30 PM

NETWORKING DRINKS AND CANAPES

WE ARE THE

CompTIA®

Community