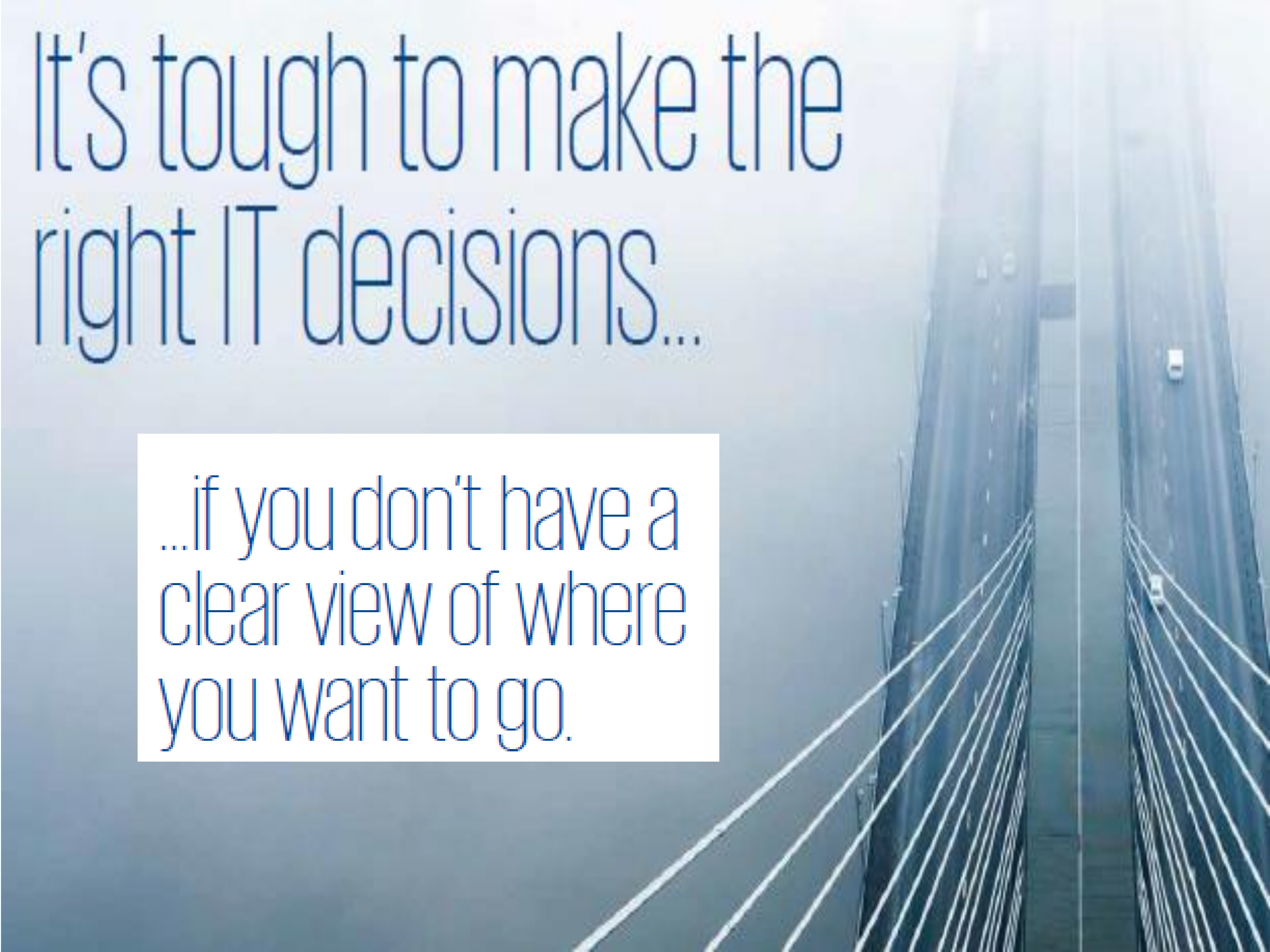
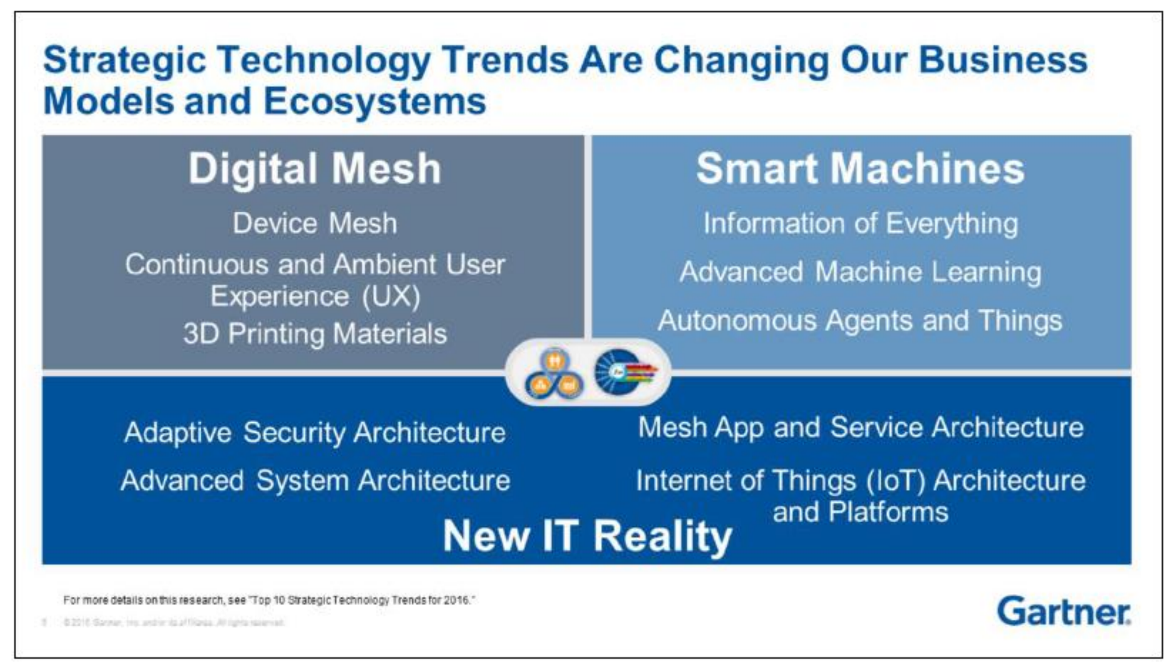
It's tough to make the right IT decisions...



...if you don't have a clear view of where you want to go.



Strategic Technology Trends Are Changing Our Business Models and Ecosystems

Digital Mesh

Device Mesh

Continuous and Ambient User Experience (UX)

3D Printing Materials

Smart Machines

Information of Everything

Advanced Machine Learning

Autonomous Agents and Things

Adaptive Security Architecture

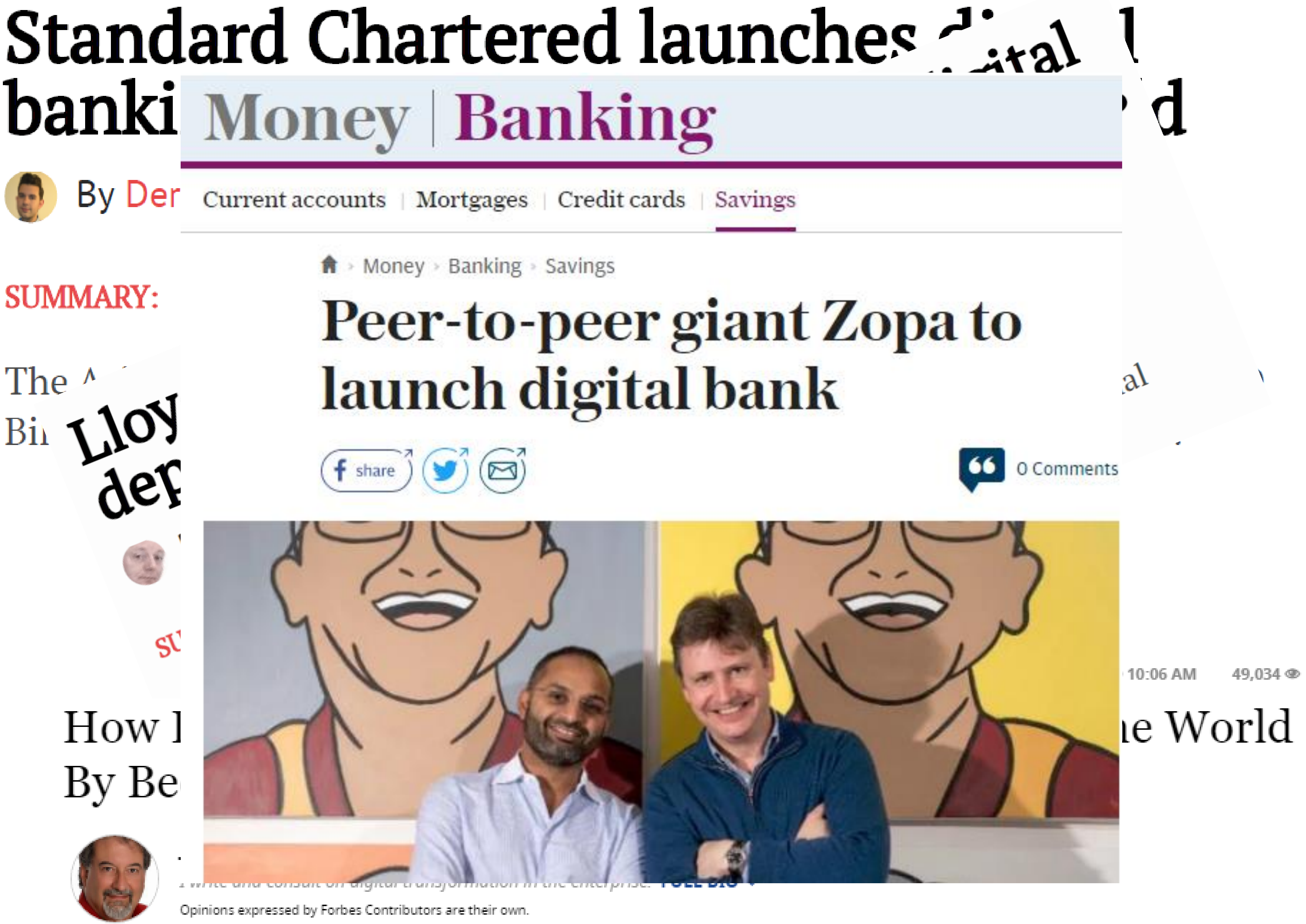
Advanced System Architecture

Mesh App and Service Architecture

Internet of Things (IoT) Architecture and Platforms

New IT Reality

For more details on this research, see "Top 10 Strategic Technology Trends for 2016."



Standard Chartered launches digital
banki d

By Der

SUMMARY:

The A
Bi

Lloy
dep

SU

al

10:06 AM 49,034

How I
By Be

e World

I write and consult on digital transformation in the enterprise. FULL BIO

Opinions expressed by Forbes Contributors are their own.

Money | Banking

Current accounts | Mortgages | Credit cards | Savings

Money › Banking › Savings

Peer-to-peer giant Zopa to launch digital bank

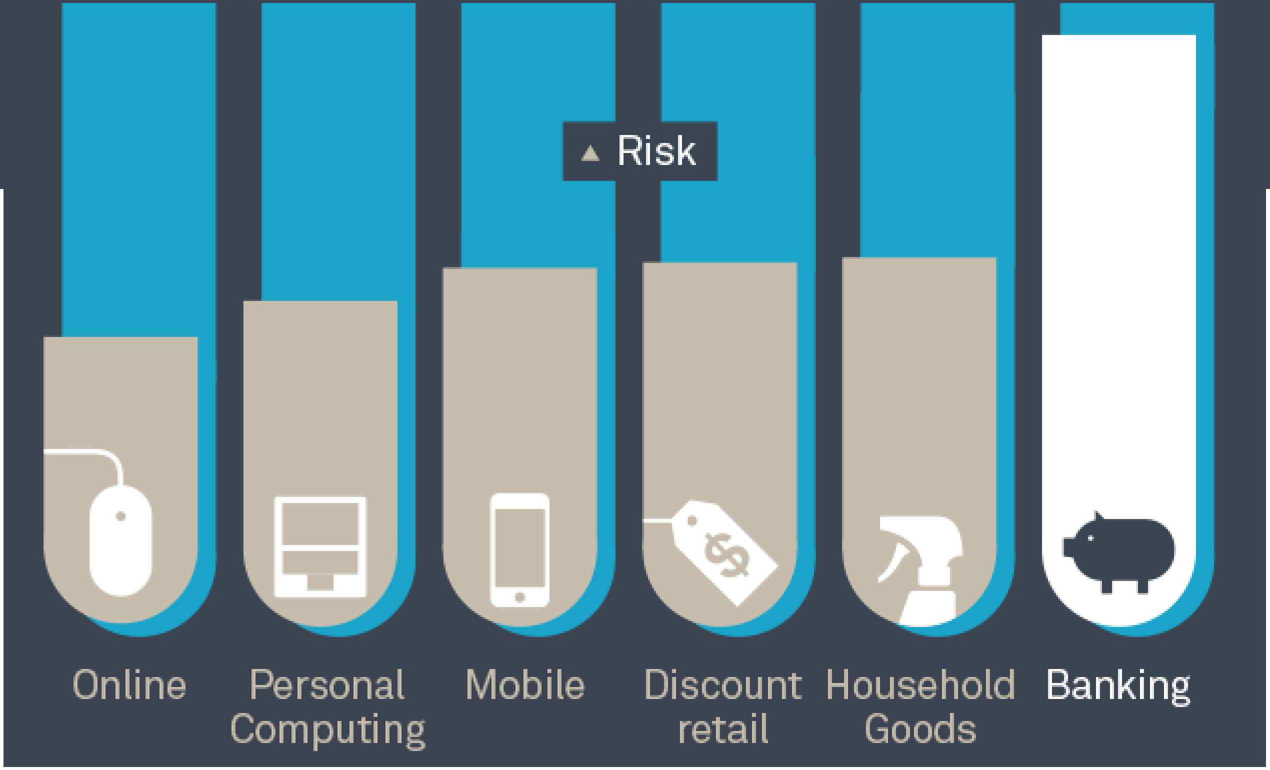
THE MILLENNIAL DISRUPTION INDEX

3 years
•
15 categories

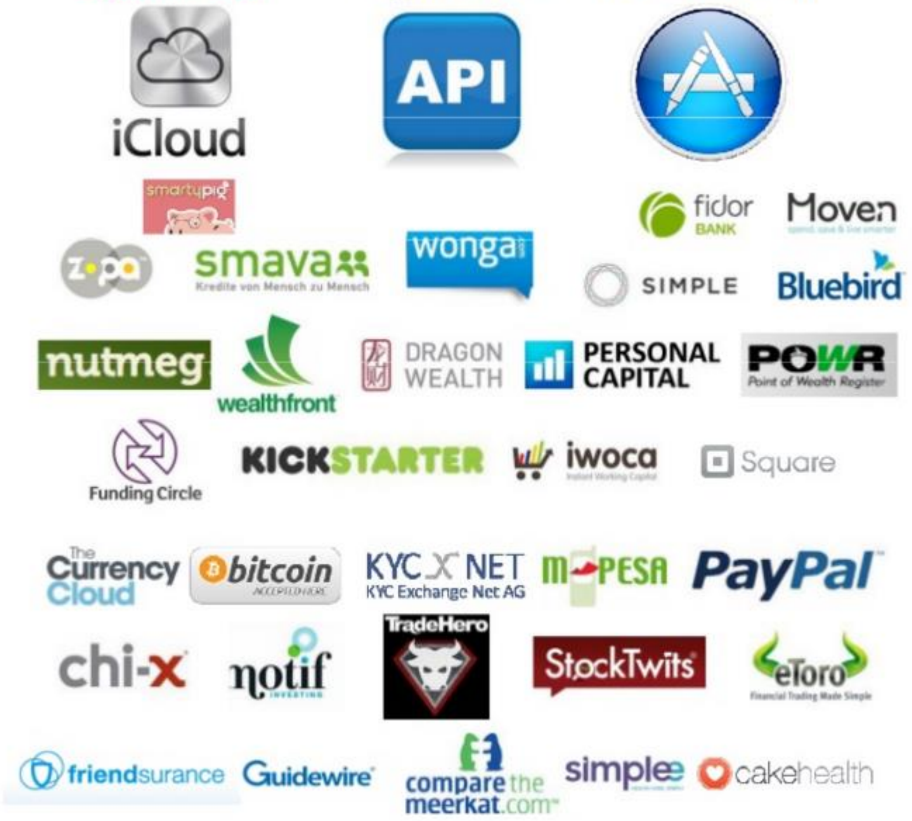
200+

10,000+

Banking is at the **highest**



Product Specialisation | **Process** Fragmentation | **People** Personalisation



Retail Banking

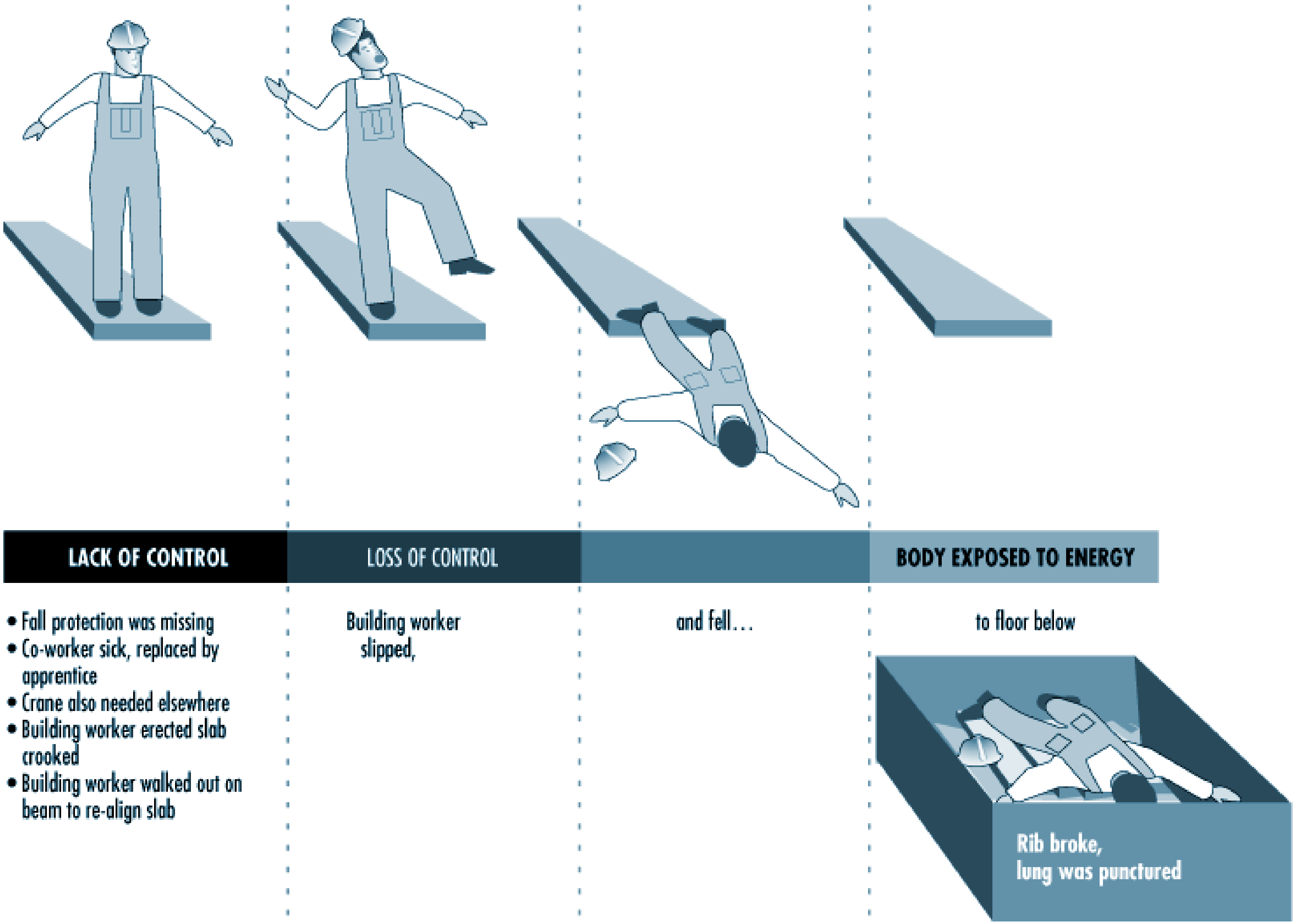
Private Banking

Commercial Banking

Transaction Banking

Investment Banking

Insurance



LACK OF CONTROL

- Fall protection was missing
- Co-worker sick, replaced by apprentice
- Crane also needed elsewhere
- Building worker erected slab crooked
- Building worker walked out on beam to re-align slab

LOSS OF CONTROL

Building worker slipped,

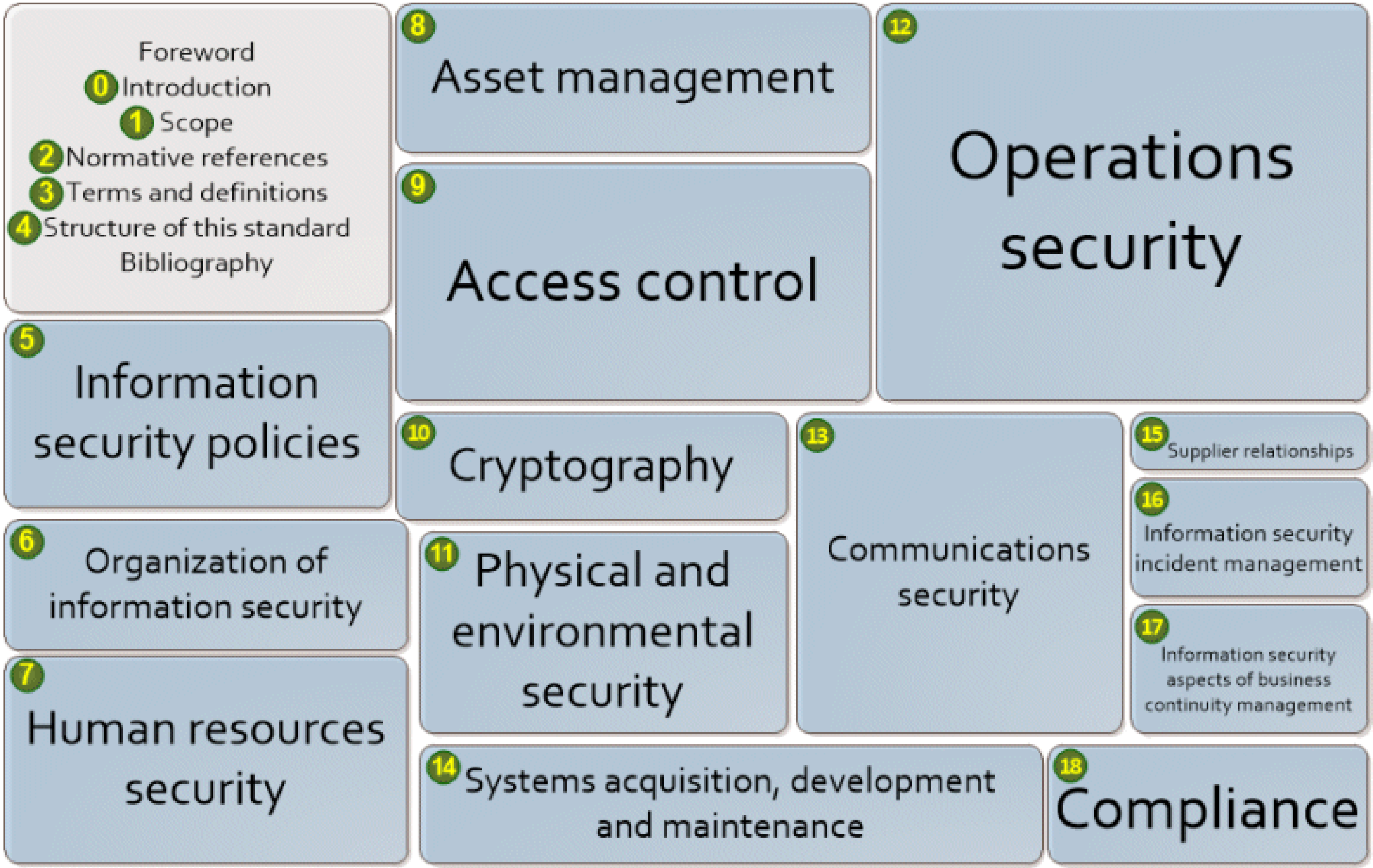
and fell…

BODY EXPOSED TO ENERGY

to floor below

Rib broke, lung was punctured

Source: Kjellén and Hovden 1993.



Foreword

0 Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Structure of this standard

Bibliography

5 Information security policies

6 Organization of information security

7 Human resources security

8 Asset management

9 Access control

10 Cryptography

11 Physical and environmental security

12 Operations security

13 Communications security

14 Systems acquisition, development and maintenance

15 Supplier relationships

16 Information security incident management

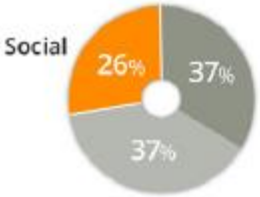
17 Information security aspects of business continuity management

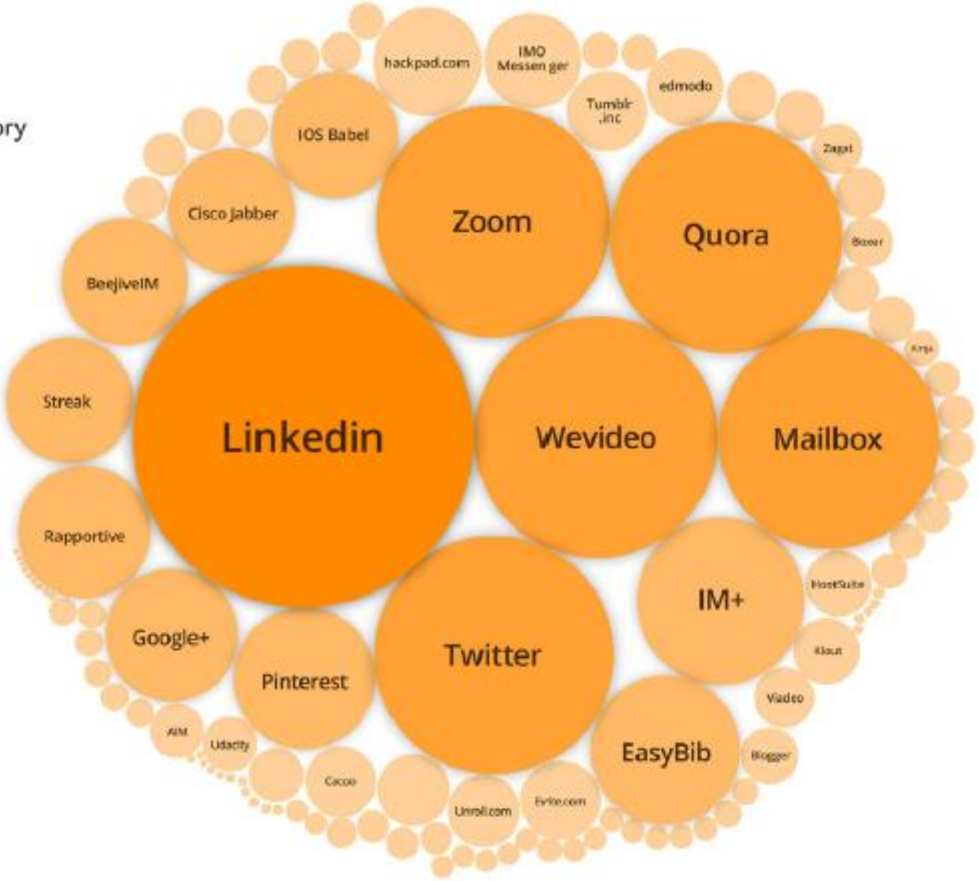
18 Compliance

Top Third-Party Apps

Social & Communication Apps

Unique Apps by Category



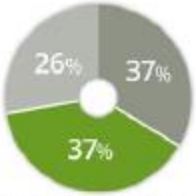


Color shows sum of total installs

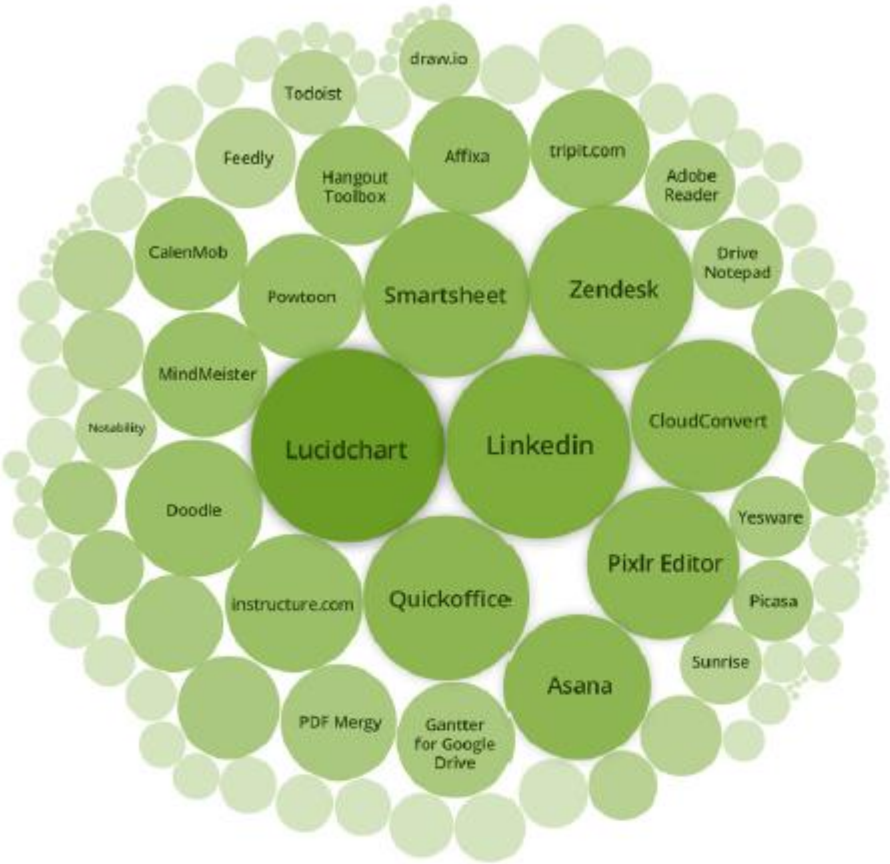
Top Third-Party Apps

Business Productivity Apps

Unique Apps by Category



Business Productivity

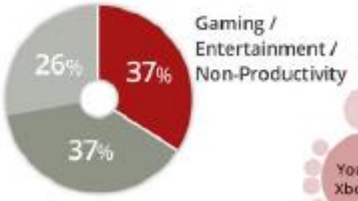


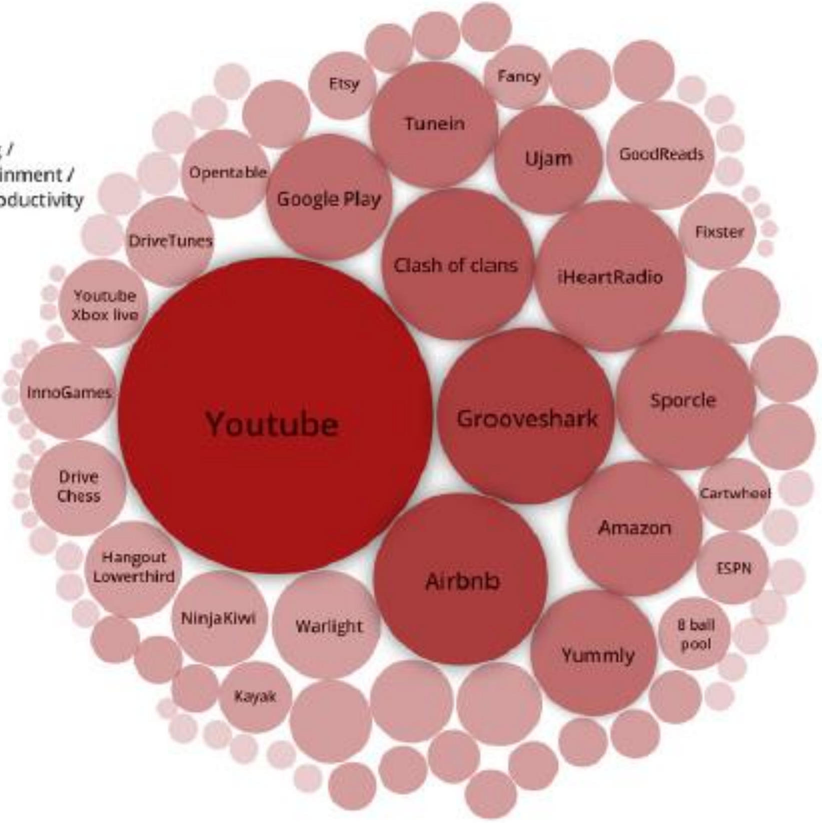
Color shows sum of total installs

Top Third-Party Apps

Gaming / Entertainment / Non-Productivity Apps

Unique Apps by Category



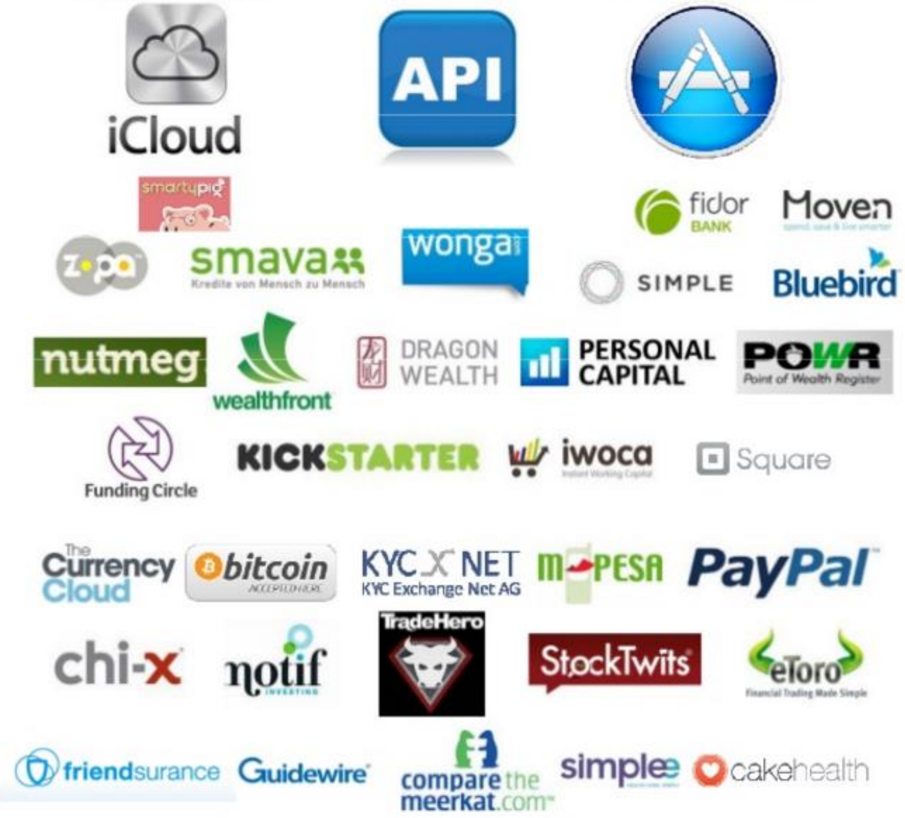


Color shows sum of total installs

Product Specialisation

Process Fragmentation

People Personalisation



Retail Banking

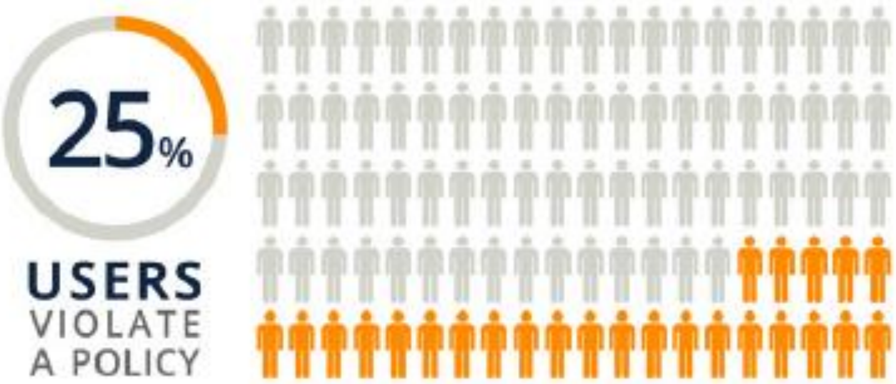
Private Banking

Commercial Banking

Transaction Banking

Investment Banking

Insurance

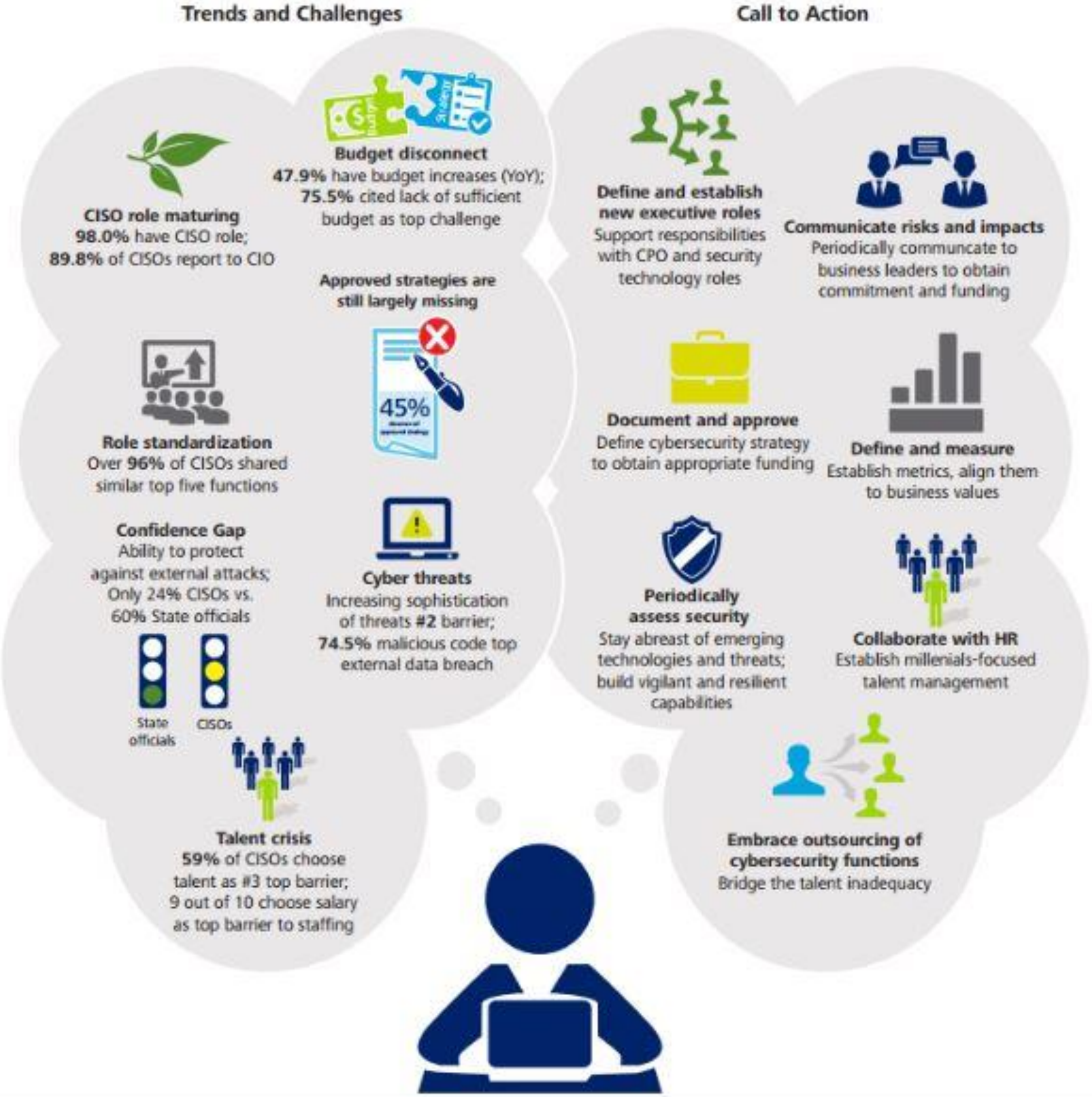


25%

USERS VIOLATE A POLICY

12%

of an organizations files are sensitive/ Violate a policy



Trends and Challenges

CISO role maturing
98.0% have CISO role;
89.8% of CISOs report to CIO

Budget disconnect
47.9% have budget increases (YoY);
75.5% cited lack of sufficient budget as top challenge

Approved strategies are still largely missing

45%

Role standardization
Over **96%** of CISOs shared similar top five functions

Confidence Gap
Ability to protect against external attacks;
Only 24% CISOs vs. 60% State officials

Cyber threats
Increasing sophistication of threats **#2** barrier;
74.5% malicious code top external data breach

Talent crisis
59% of CISOs choose talent as #3 top barrier;
9 out of 10 choose salary as top barrier to staffing

Call to Action

Define and establish new executive roles
Support responsibilities with CPO and security technology roles

Communicate risks and impacts
Periodically communcate to business leaders to obtain commitment and funding

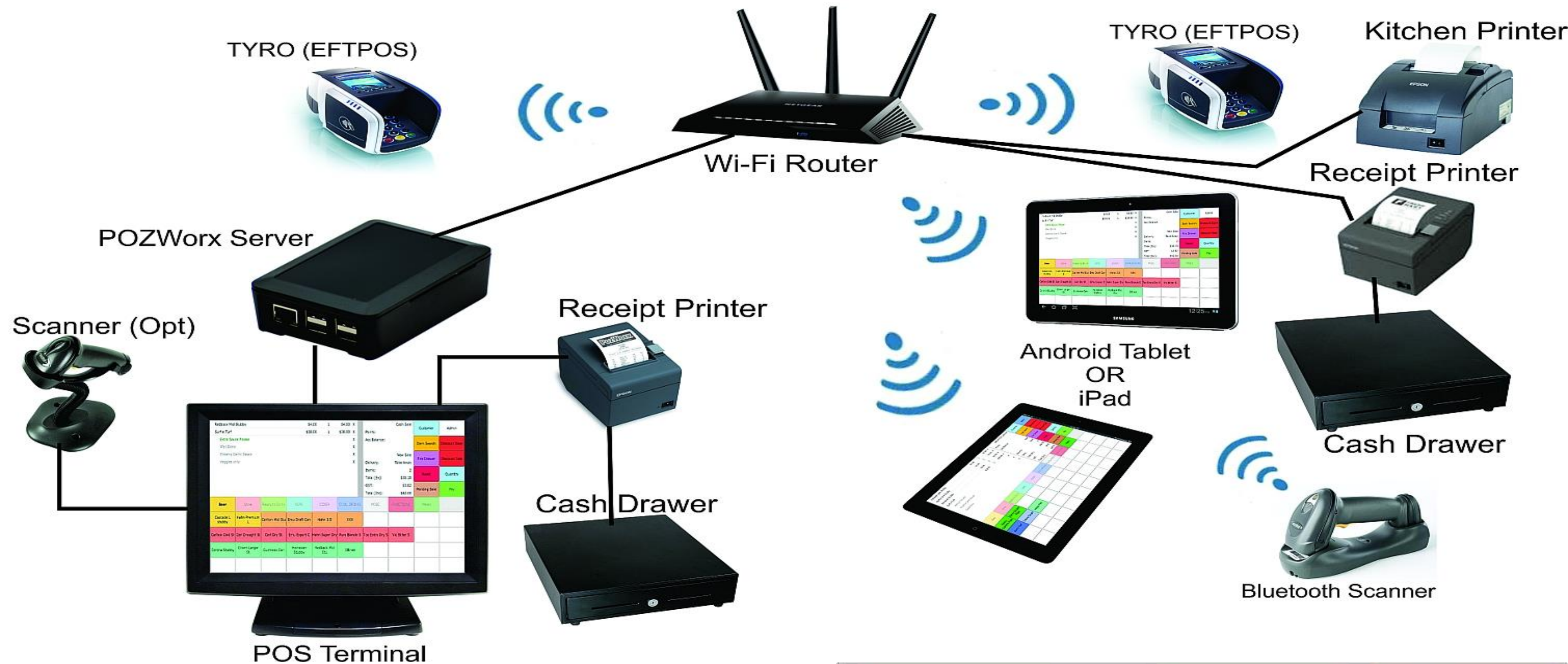
Document and approve
Define cybersecurity strategy to obtain appropriate funding

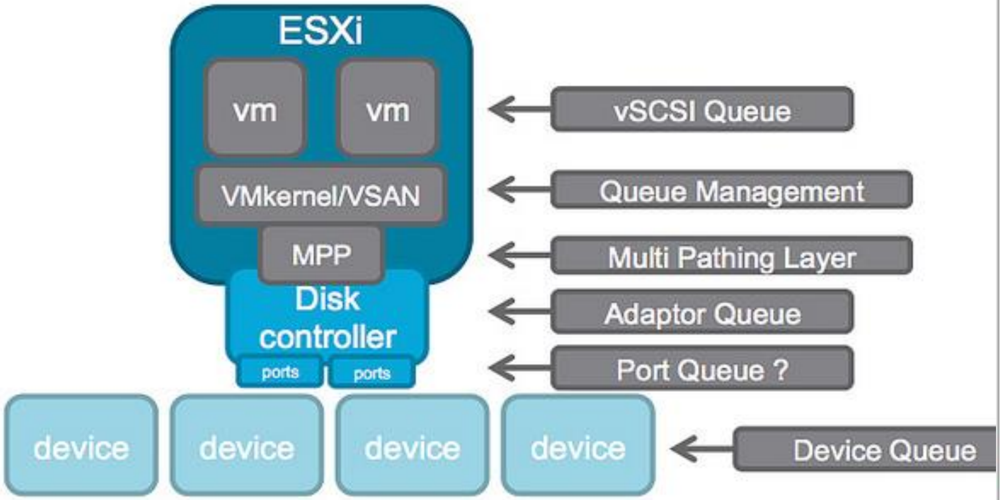
Define and measure
Establish metrics, align them to business values

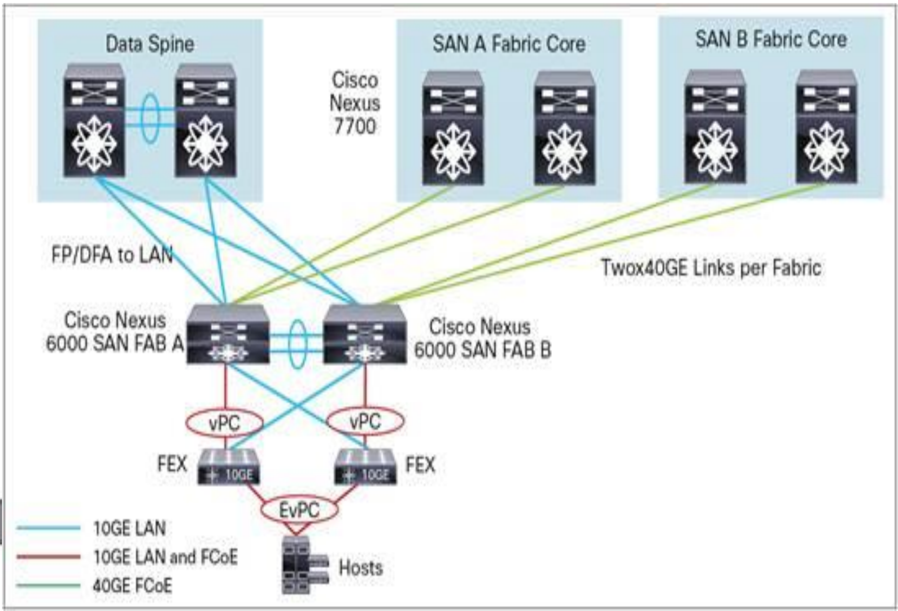
Periodically assess security
Stay abreast of emerging technologies and threats; build vigilant and resilient capabilities

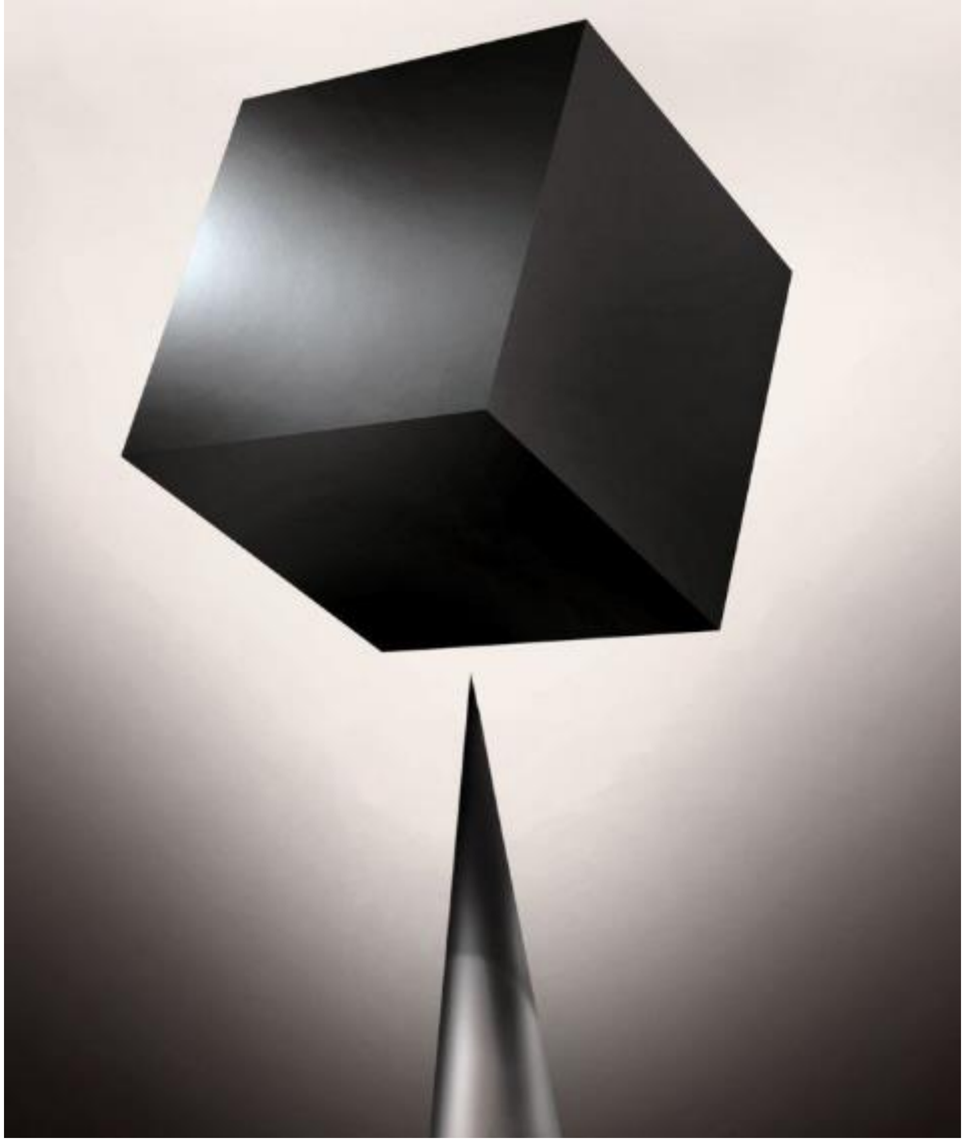
Collaborate with HR
Establish millenials-focused talent management

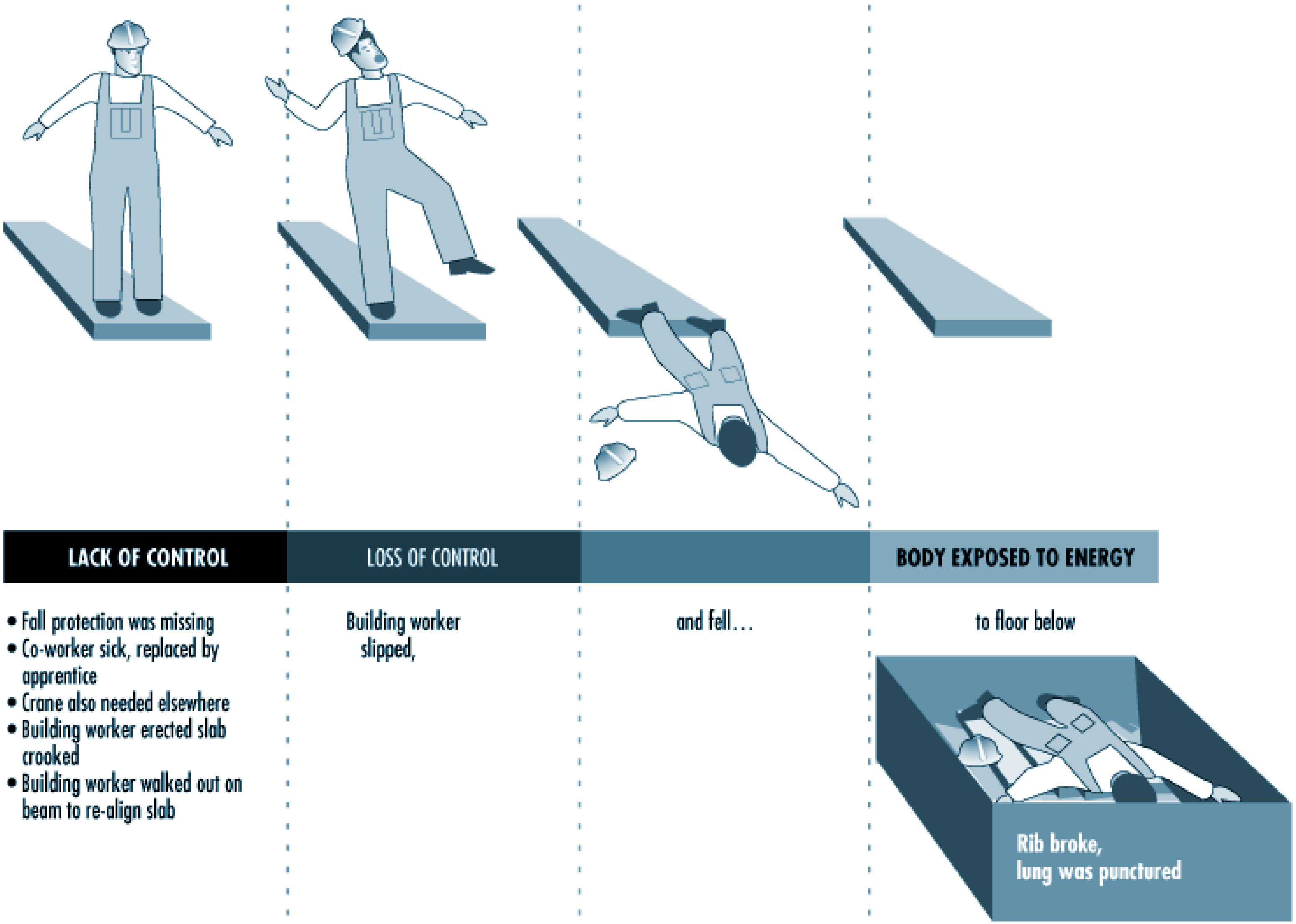
Embrace outsourcing of cybersecurity functions
Bridge the talent inadequacy


TYRO (EFTPOS)
Wi-Fi Router
TYRO (EFTPOS)
Kitchen Printer
Receipt Printer
POZWorx Server
Scanner (Opt)
Receipt Printer
Android Tablet
OR
iPad
Cash Drawer
Cash Drawer
Bluetooth Scanner
POS Terminal


ESXi
vm
vm
VMkernel/VSAN
MPP
Disk controller
ports
ports
device
device
device
device
vSCSI Queue
Queue Management
Multi Pathing Layer
Adaptor Queue
Port Queue ?
Device Queue

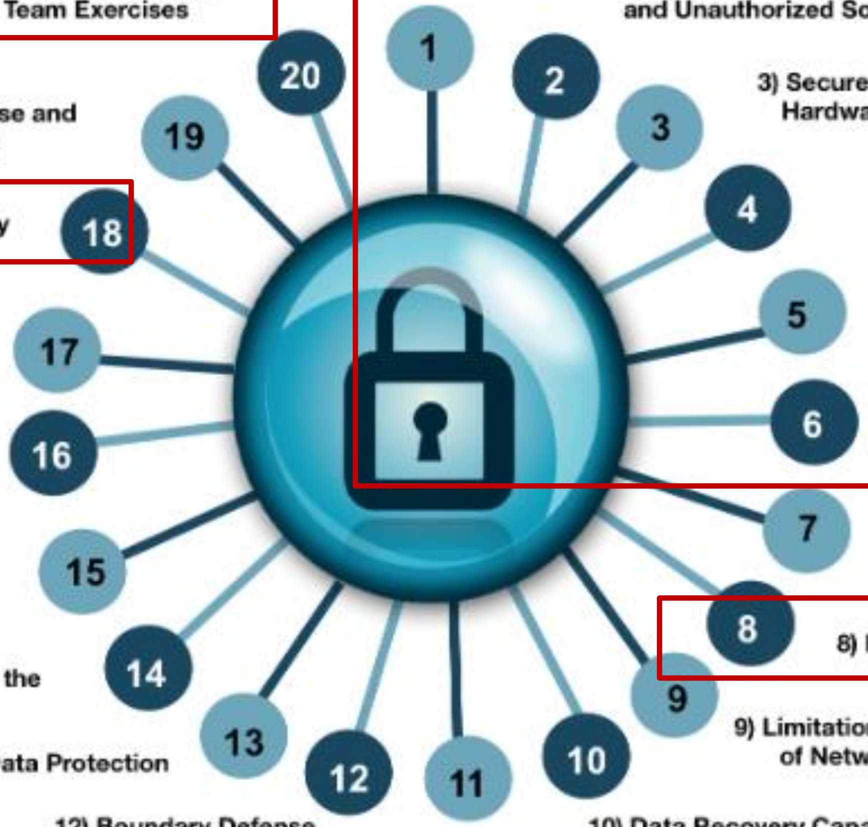

Data Spine
Cisco Nexus 7700
SAN A Fabric Core
SAN B Fabric Core
FP/DFA to LAN
Twox40GE Links per Fabric
Cisco Nexus 6000 SAN FAB A
Cisco Nexus 6000 SAN FAB B
vPC
vPC
FEX
10GE
FEX
10GE
EvPC
Hosts
10GE LAN
10GE LAN and FCoE
40GE FCoE




LACK OF CONTROL
LOSS OF CONTROL
BODY EXPOSED TO ENERGY
• Fall protection was missing
• Co-worker sick, replaced by apprentice
• Crane also needed elsewhere
• Building worker erected slab crooked
• Building worker walked out on beam to re-align slab
Building worker slipped,
and fell…
to floor below
Rib broke, lung was punctured

Source: Kjellén and Hovden 1993.

CIS Critical Security Controls



1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

4) Continuous Vulnerability Assessment and Remediation

5) Controlled Use of Administrative Privileges

6) Maintenance, Monitoring and Analysis of Audit Logs

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports

10) Data Recovery Capability

11) Secure Configurations for Network Devices

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

16) Account Monitoring and Control

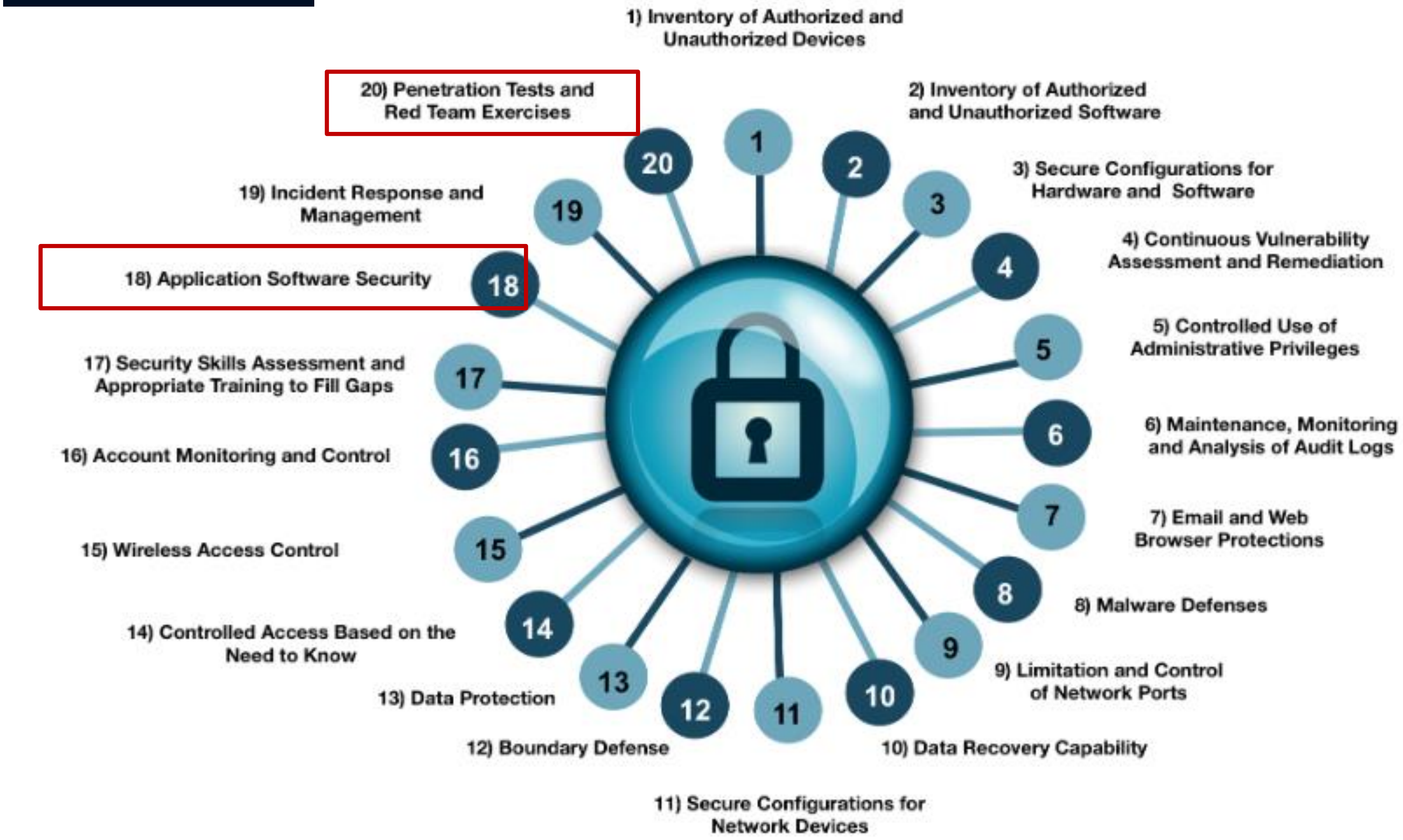
17) Security Skills Assessment and Appropriate Training to Fill Gaps

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises

CIS Critical Security Controls



1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

4) Continuous Vulnerability Assessment and Remediation

5) Controlled Use of Administrative Privileges

6) Maintenance, Monitoring and Analysis of Audit Logs

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports

10) Data Recovery Capability

11) Secure Configurations for Network Devices

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

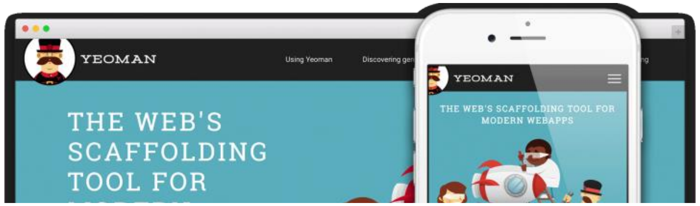
16) Account Monitoring and Control

17) Security Skills Assessment and Appropriate Training to Fill Gaps

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises


YEOMAN
Using Yeoman
Discovering ger
THE WEB'S SCAFFOLDING TOOL FOR
YEOMAN
THE WEB'S SCAFFOLDING TOOL FOR MODERN WEBAPPS

Deliver, Service and Support (DSS)

Manage Business Process Controls

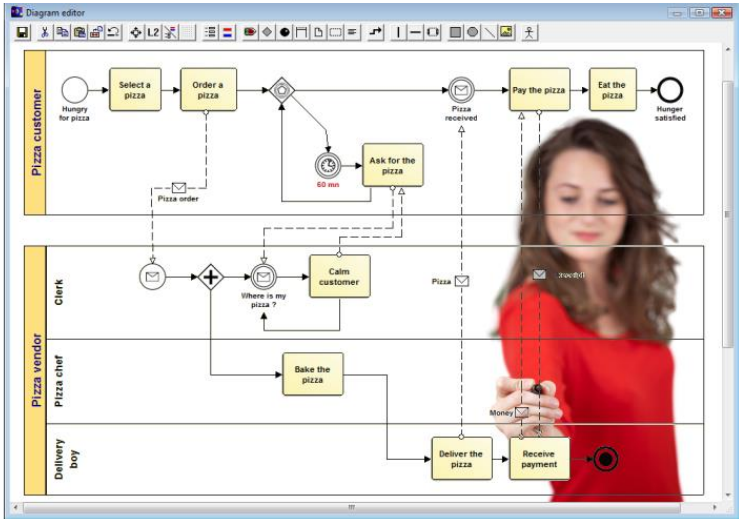
DSS06 Manage Business Process Controls

Process Description
Define and maintain appropriate business proc
to and processed by in-house or outsourced bu
information control requirements. Identify the r
manage and operate adequate controls to ens
satisfy these requirements.

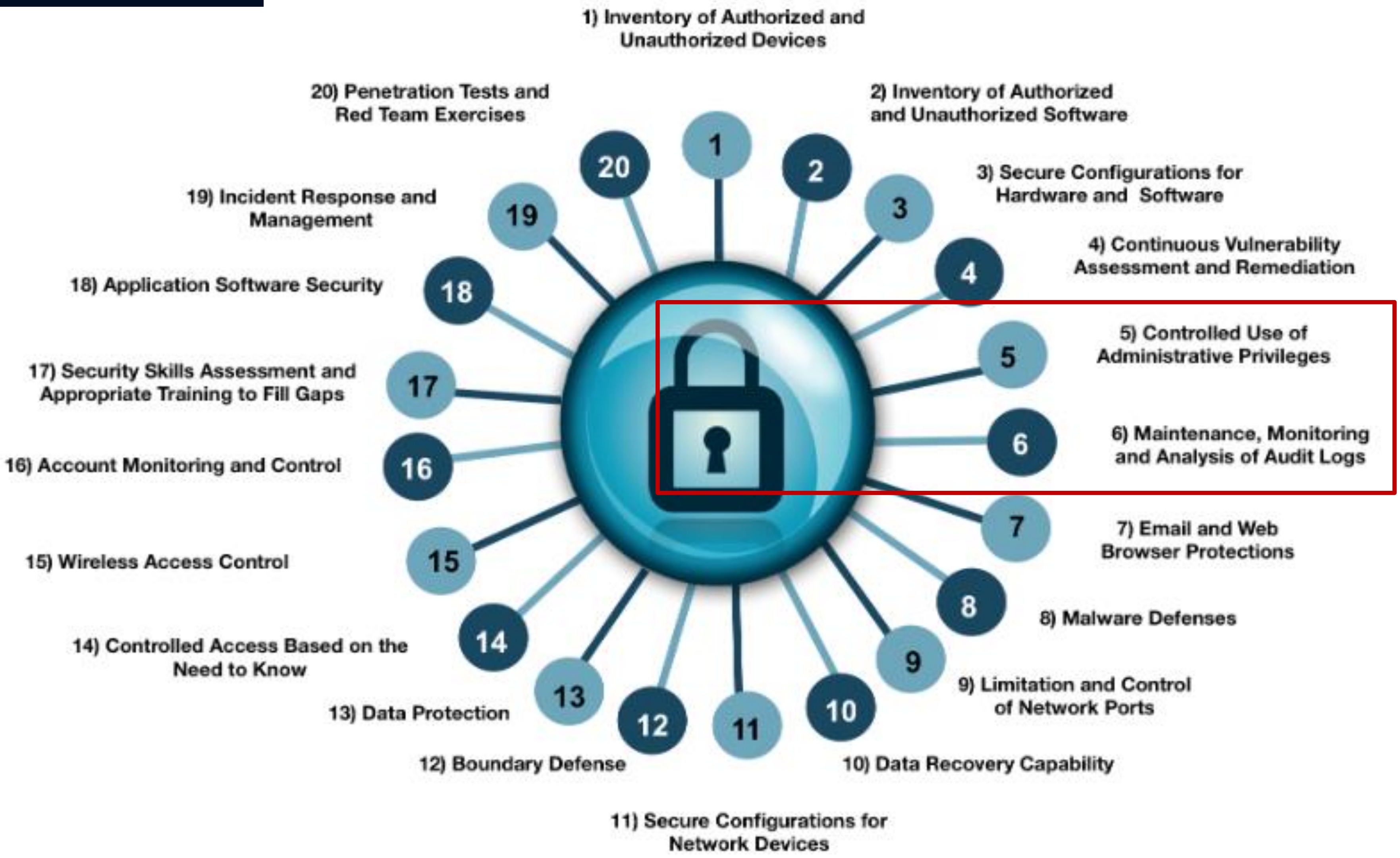
Process Purpose Statement
Maintain information integrity and the security
processes in the enterprise or outsourced.

COBIT 5

Key Governance Practice	Board	Chief Execu	Chief Financ	Chief Opera	Business Ex	Business Pro	Strategy Ex	Steering (Pr	Committee Project Man	Value Mana	Chief Risk O	Chief Inform
DSS06.01 Align control activities embedded in business processes with enterprise objectives.		C	C	C	A	R					I	I
DSS06.02 Control the processing of information.		R	R	R	A	R					I	I
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.			R		A	R						I
DSS06.04 Manage errors and exceptions.				I	I	A						
DSS06.05 Ensure traceability of Information events and accountabilities.					C	A						I



CIS Critical Security Controls



1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

4) Continuous Vulnerability Assessment and Remediation

5) Controlled Use of Administrative Privileges

6) Maintenance, Monitoring and Analysis of Audit Logs

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports

10) Data Recovery Capability

11) Secure Configurations for Network Devices

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

16) Account Monitoring and Control

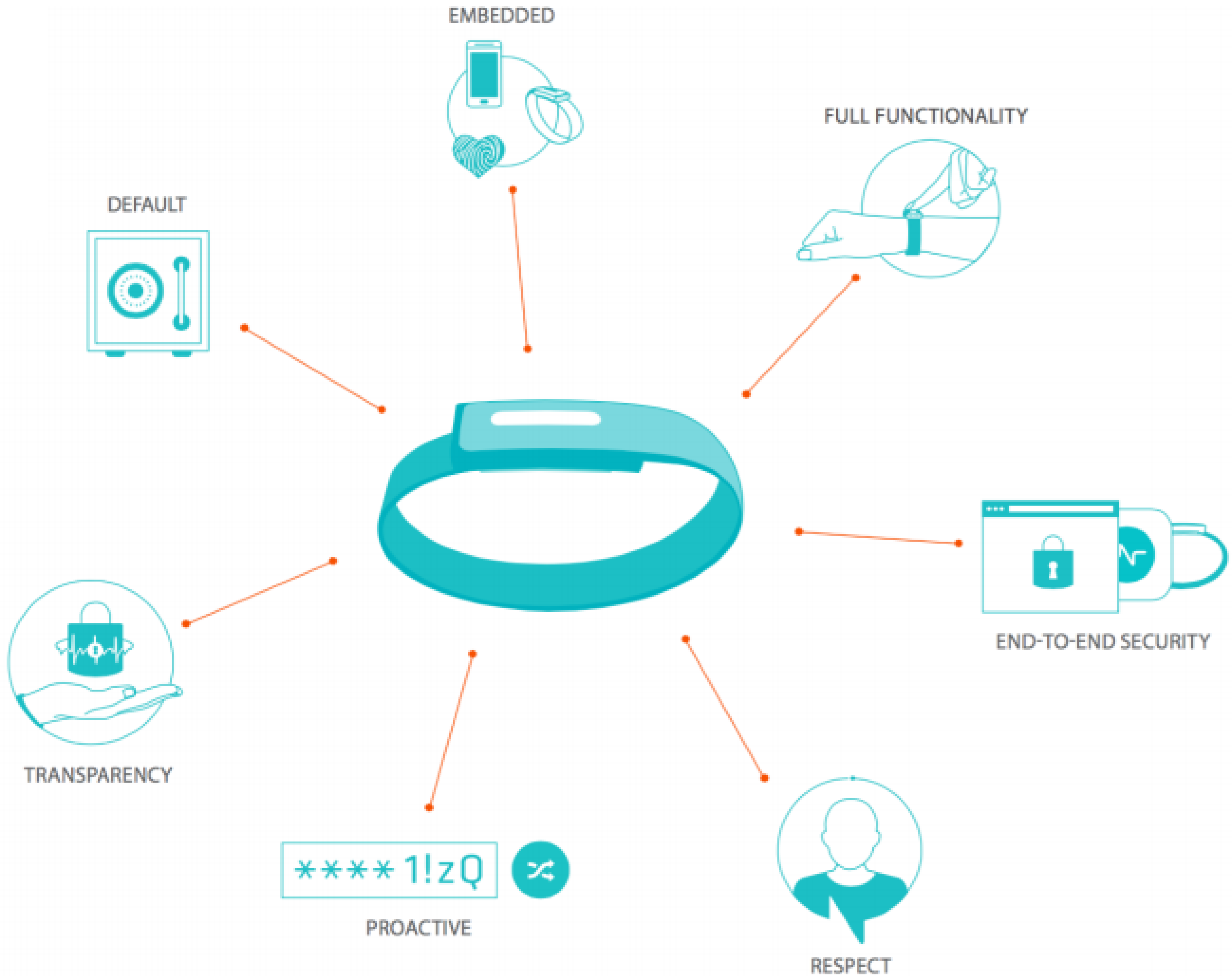
17) Security Skills Assessment and Appropriate Training to Fill Gaps

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises

Multi-Factor Authentication



EMBEDDED

FULL FUNCTIONALITY

DEFAULT

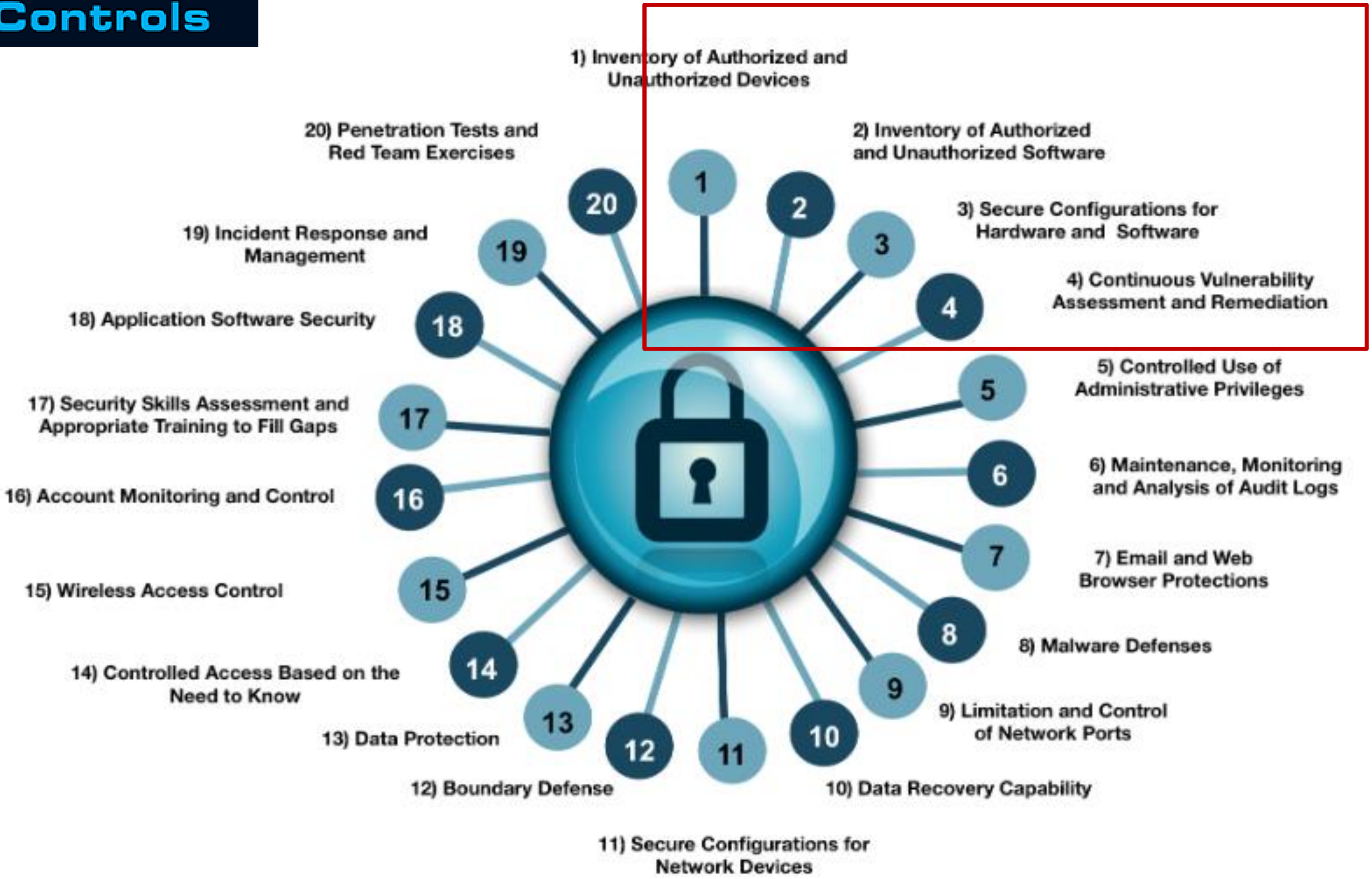
END-TO-END SECURITY

TRANSPARENCY

PROACTIVE

RESPECT

CIS Critical Security Controls



1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

4) Continuous Vulnerability Assessment and Remediation

5) Controlled Use of Administrative Privileges

6) Maintenance, Monitoring and Analysis of Audit Logs

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports

10) Data Recovery Capability

11) Secure Configurations for Network Devices

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

16) Account Monitoring and Control

17) Security Skills Assessment and Appropriate Training to Fill Gaps

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises

HARDEN YOUR SYSTEMS

PROTECT YOUR DATA

PATCH FATIGUE

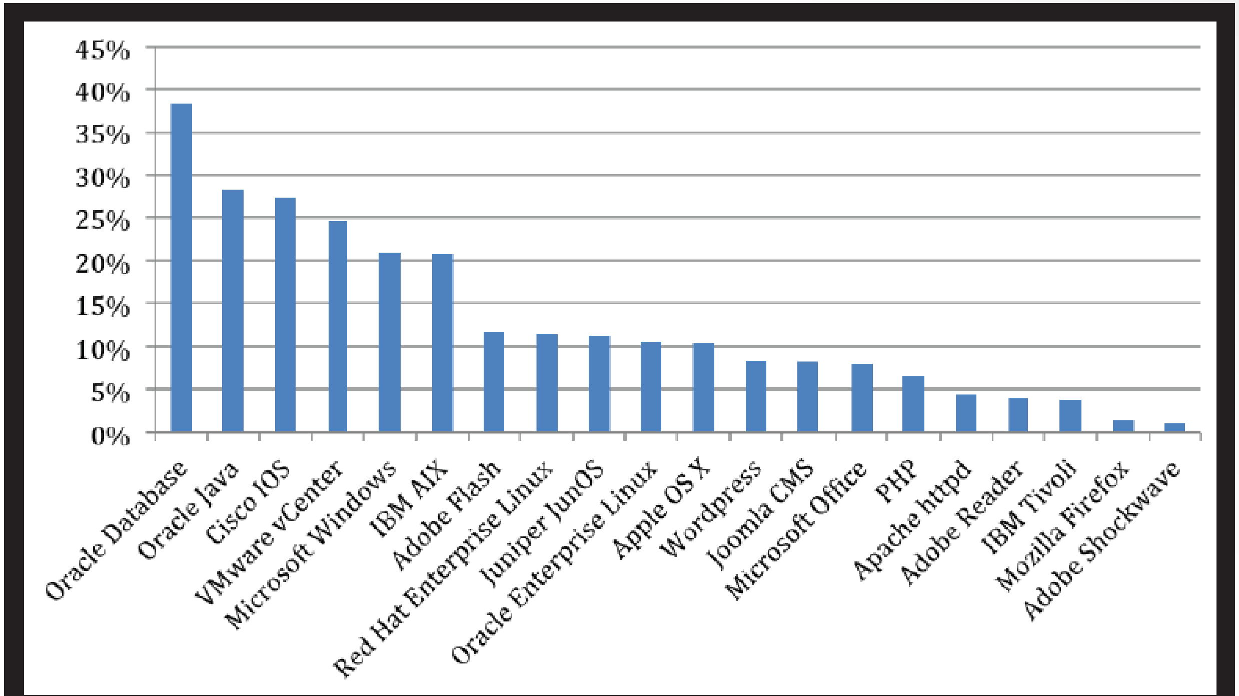
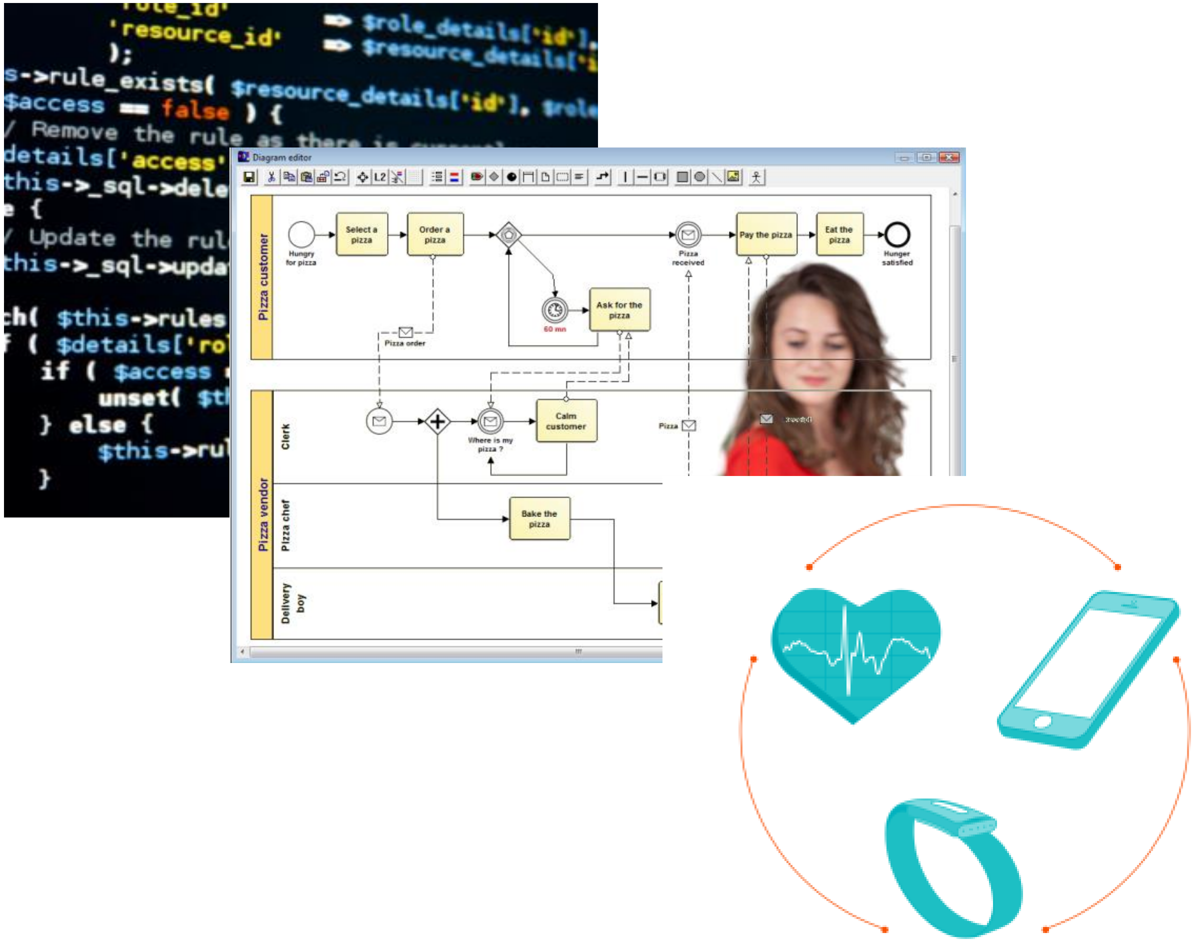


FIG. 3 *Rank of platforms by patching difficulty*

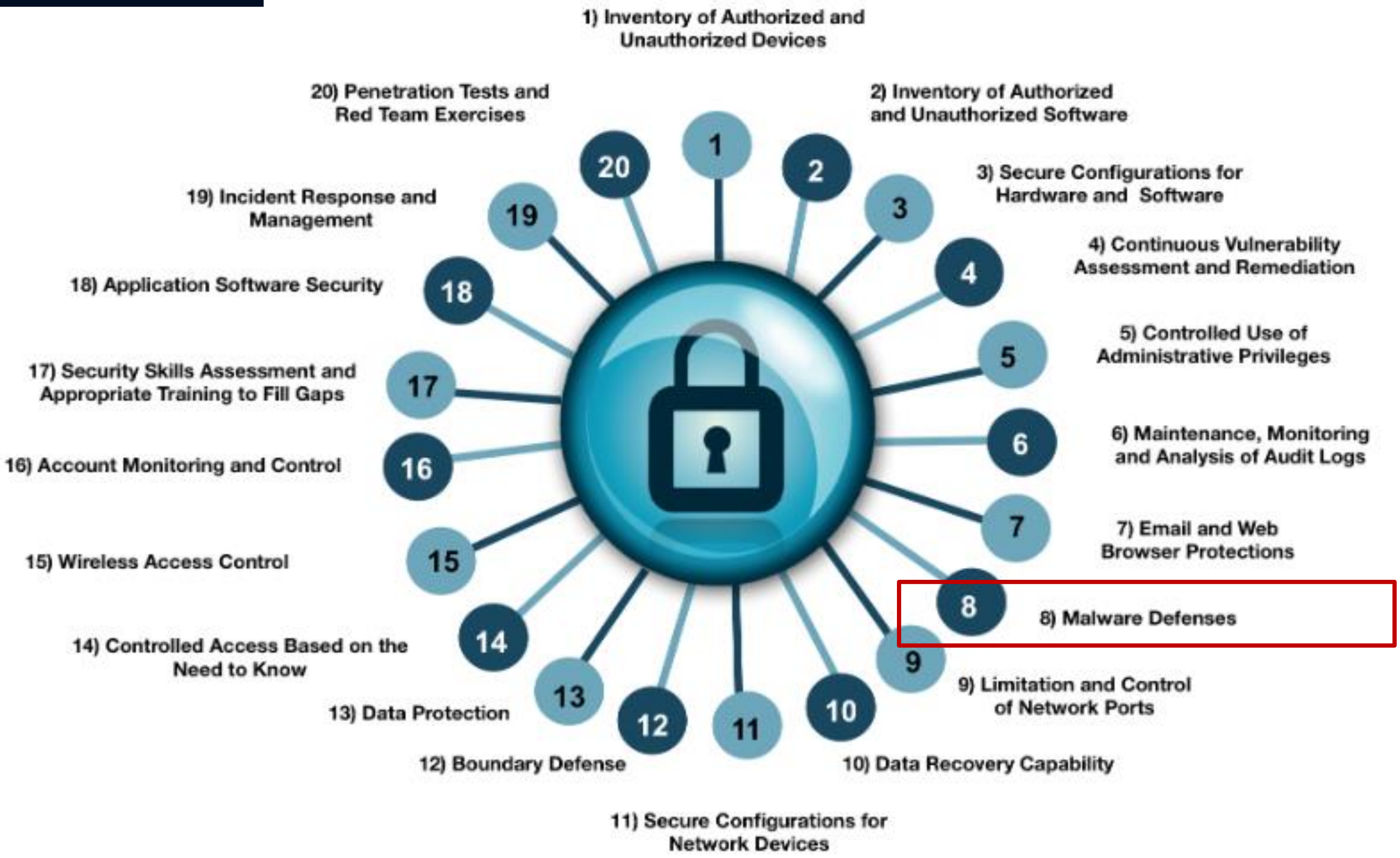


```
             role_id'
            'resource_id'      => $role_details['id'],
            );                 => $resource_details['i
s->rule_exists( $resource_details['id'], $role
$access == false ) {
/ Remove the rule as there is current
details['access'
this->_sql->dele
e {
/ Update the rul
this->_sql->upda

ch( $this->rules
f ( $details['ro
    if ( $access
        unset( $th
    } else {
        $this->rul
    }
```

HARDEN
YOUR
SYSTEMS
PROTECT
YOUR
DATA

CIS Critical Security Controls



1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

4) Continuous Vulnerability Assessment and Remediation

5) Controlled Use of Administrative Privileges

6) Maintenance, Monitoring and Analysis of Audit Logs

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports

10) Data Recovery Capability

11) Secure Configurations for Network Devices

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

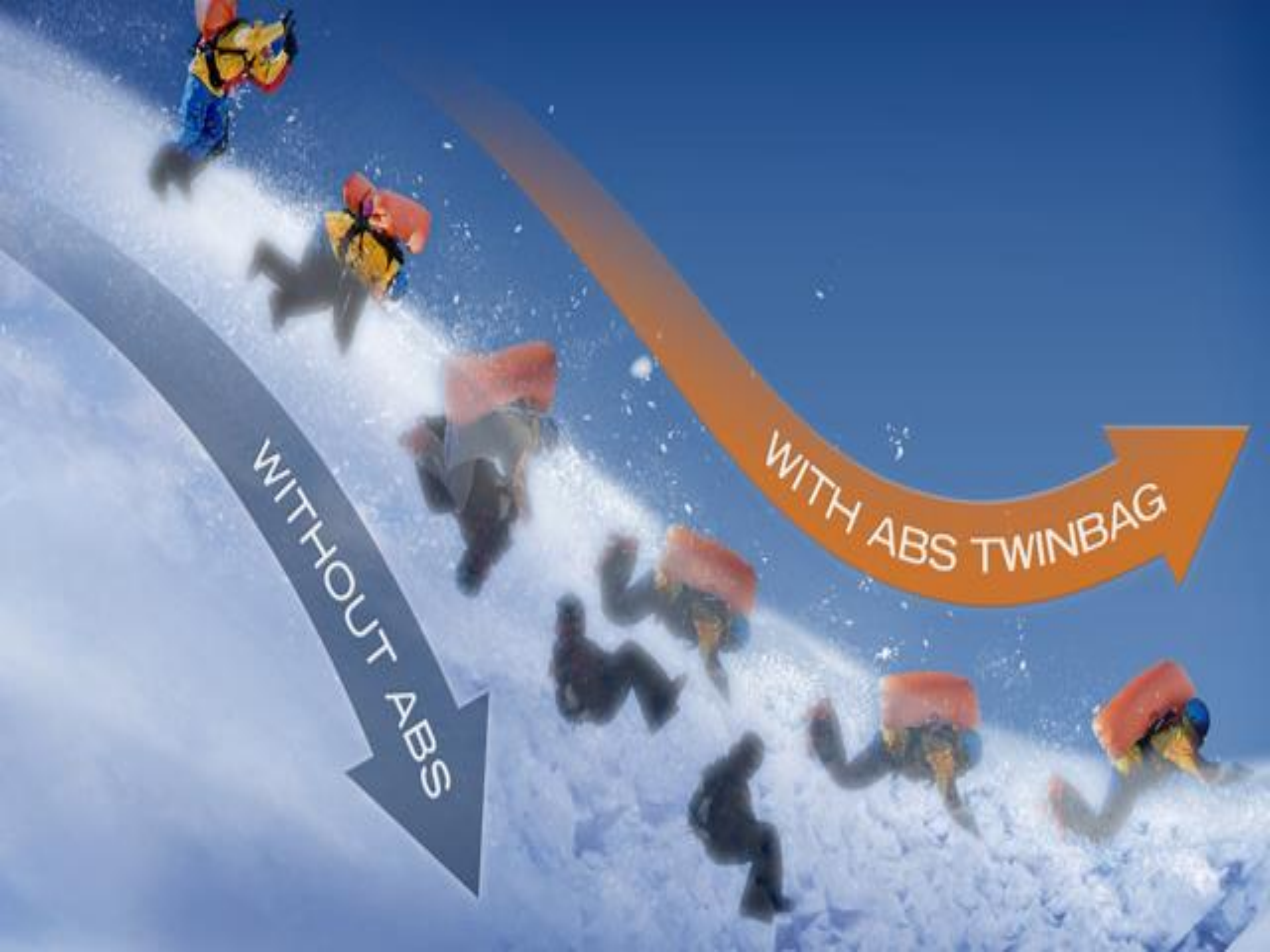
16) Account Monitoring and Control

17) Security Skills Assessment and Appropriate Training to Fill Gaps

18) Application Software Security

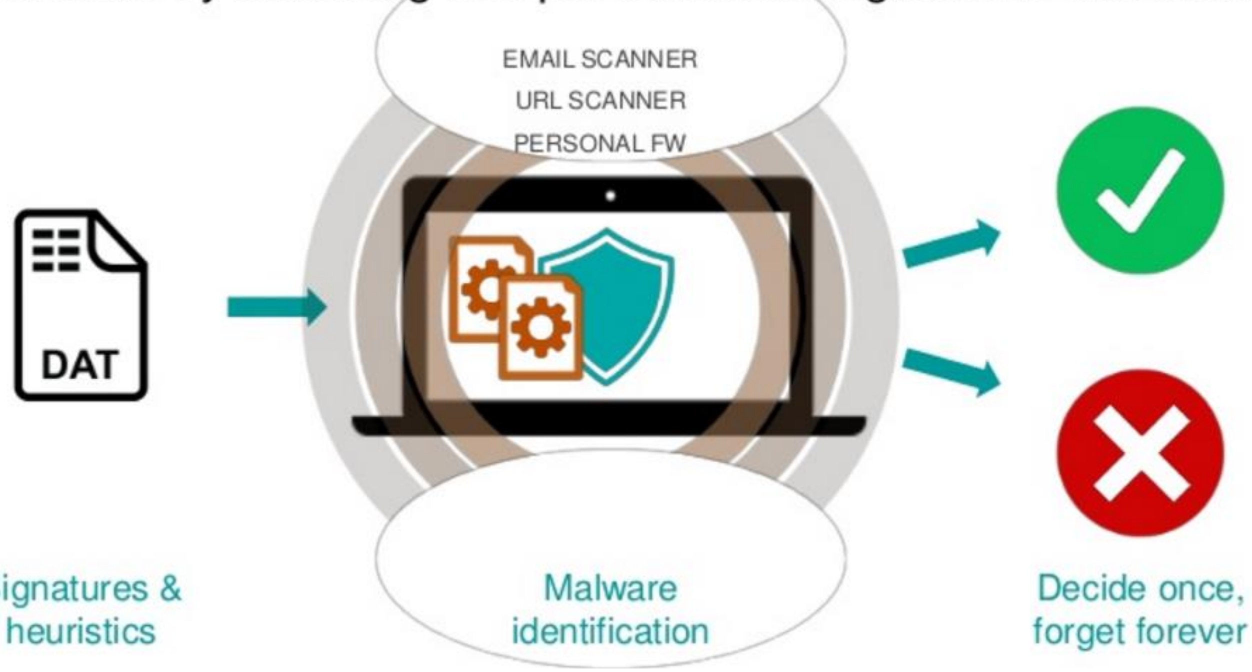
19) Incident Response and Management

20) Penetration Tests and Red Team Exercises


WITHOUT ABS
WITH ABS TWINBAG

TRADITIONAL ANTIVIRUS

Traditional AV takes a **malware-centric view** of endpoint security; identifying malicious software by matching it to pre-identified signatures and heuristics.



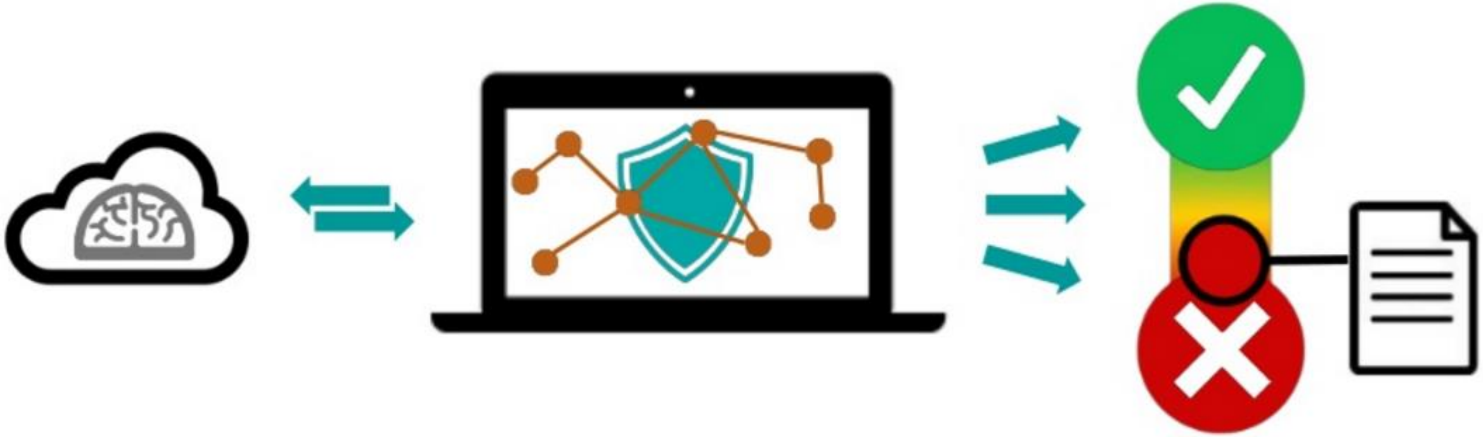
Signatures & heuristics

Malware identification

Decide once, forget forever

NEXT-GENERATION ANTIVIRUS

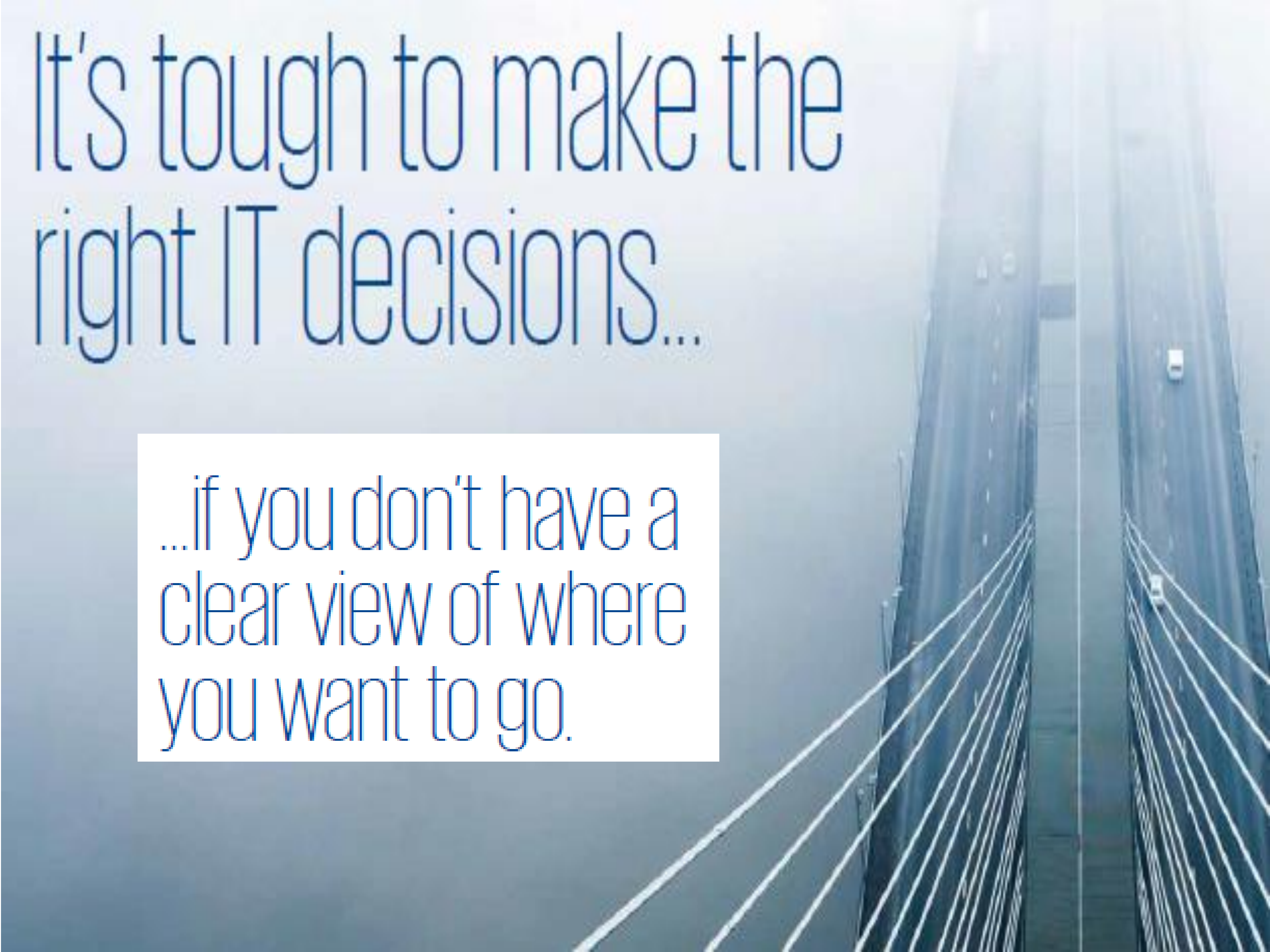
NGAV takes a **system-centric view of endpoint security**, examining every process on every endpoint to algorithmically detect and block the malicious **tools, tactics, techniques, and procedures** upon which attackers rely.



Data science & threat intelligence

Long-term analysis to detect attacker patterns

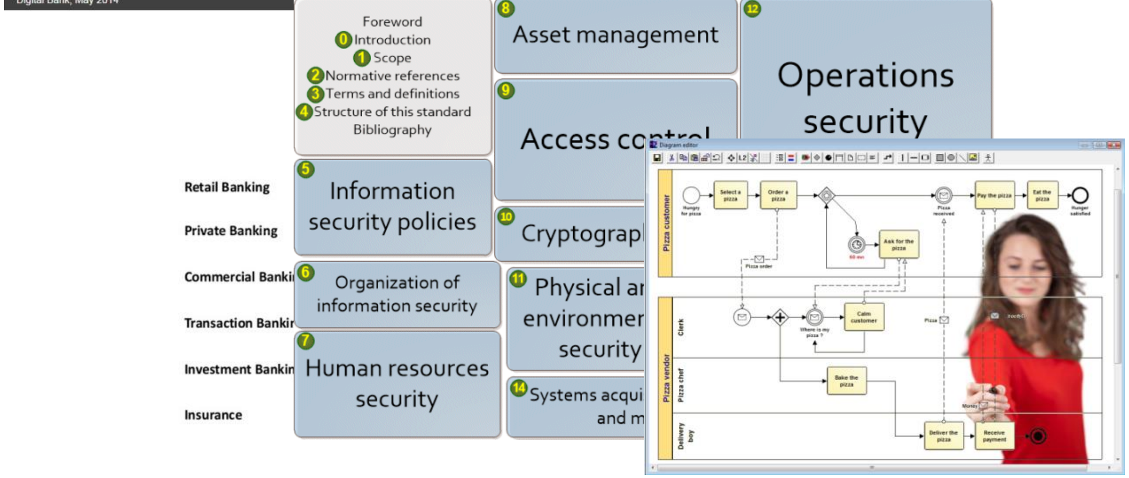
Deep attack context & insight

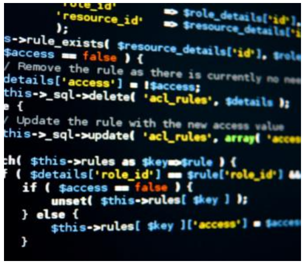


It's tough to make the right IT decisions...

...if you don't have a clear view of where you want to go.

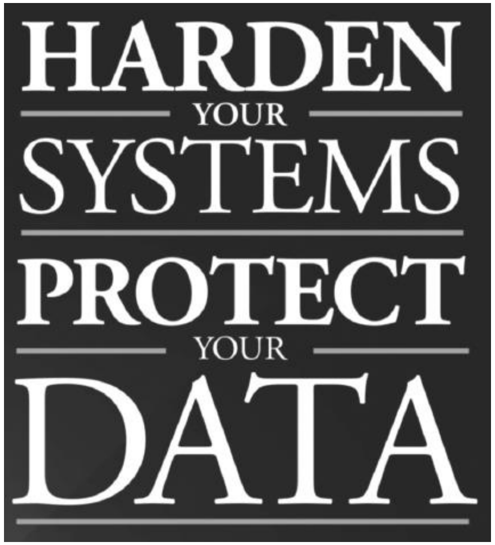
To Summarize



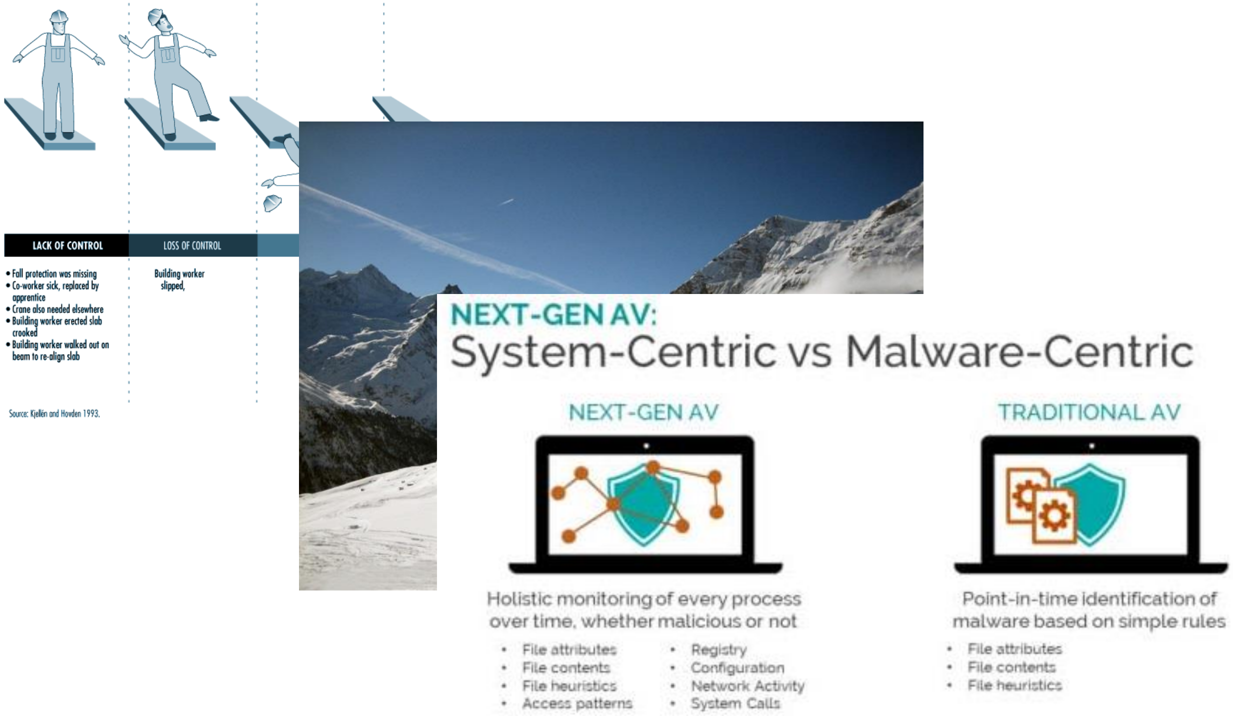


```
        'role_id'        => $role_details['id'],
        'resource_id'    => $resource_details['i
        );
s->rule_exists( $resource_details['id'], $role
$access == false ) {
/ Remove the rule as there is currently no nee
details['access'] = !$access;
this->_sql->delete( 'acl_rules', $details );
e {
/ Update the rule with the new access value
this->_sql->update( 'acl_rules', array( 'acces

ch( $this->rules as $key=>$rule ) {
f ( $details['role_id'] == $rule['role_id'] &&
  if ( $access == false ) {
      unset( $this->rules[ $key ] );
  } else {
      $this->rules[ $key ]['access'] = $acces
  }
```



HARDEN
YOUR
SYSTEMS
PROTECT
YOUR
DATA



LACK OF CONTROL

- Fall protection was missing
- Co-worker sick, replaced by apprentice
- Crane also needed elsewhere
- Building worker erected slab crooked
- Building worker walked out on beam to re-align slab

LOSS OF CONTROL

Building worker slipped,

Source: Kjellén and Hovden 1993.

NEXT-GEN AV:
System-Centric vs Malware-Centric

NEXT-GEN AV

Holistic monitoring of every process over time, whether malicious or not

- File attributes
- File contents
- File heuristics
- Access patterns
- Registry
- Configuration
- Network Activity
- System Calls

TRADITIONAL AV

Point-in-time identification of malware based on simple rules

- File attributes
- File contents
- File heuristics

f9
(
9
)
0
–
-
+
=
T
H
A
N
K
Y
O
U
return
<
>
?
/