OCEAN OUTCOMES
Fish | Food | Livelihoods

Simple low-budget and low-tech steps to ensure security for a virtual workforce

Perry Broderick

23 September 2019

PollEv.com/perryb188

Agenda:

Speak about O2

Cloud services and nonprofits

Best practices in cloud services use

Goals:

Leverage O2 experience as a fully transparent case study

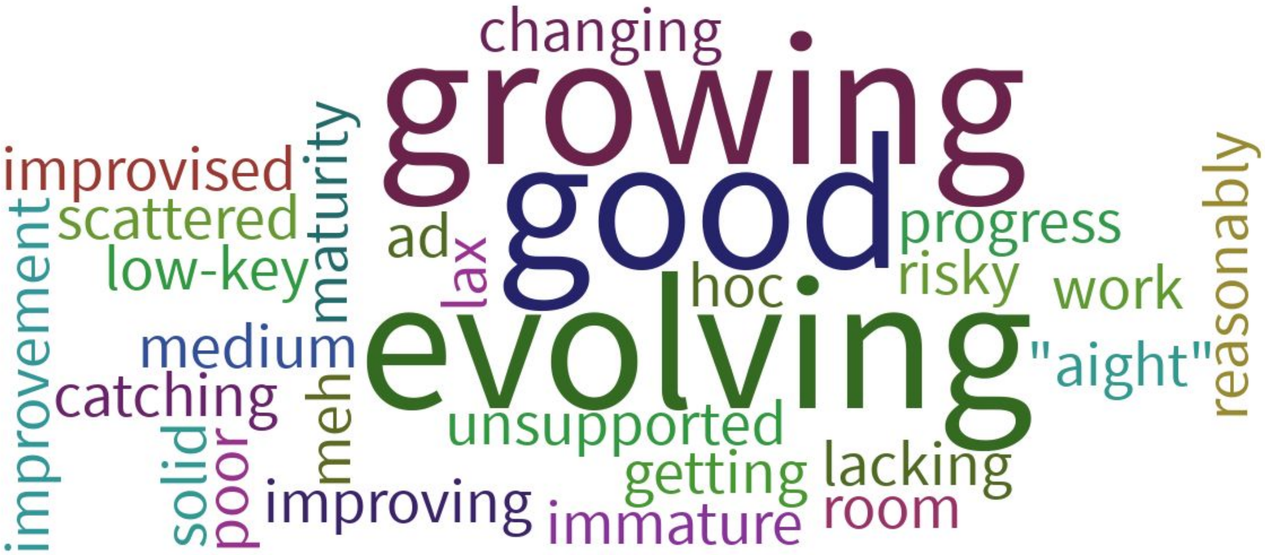
Review of best practices in cloud services security

Generate enthusiasm towards improving security

How would you describe your organization's IT environment and its security?

ⓘ Poll is full and no longer accepting responses

How would you describe your organization's IT environment and its security?



Poll Everywhere

OCEAN OUTCOMES

SUSTAINABLE FISHERIES

100% VIRTUAL

100% BYOD

16 USERS IN 7 COUNTRIES

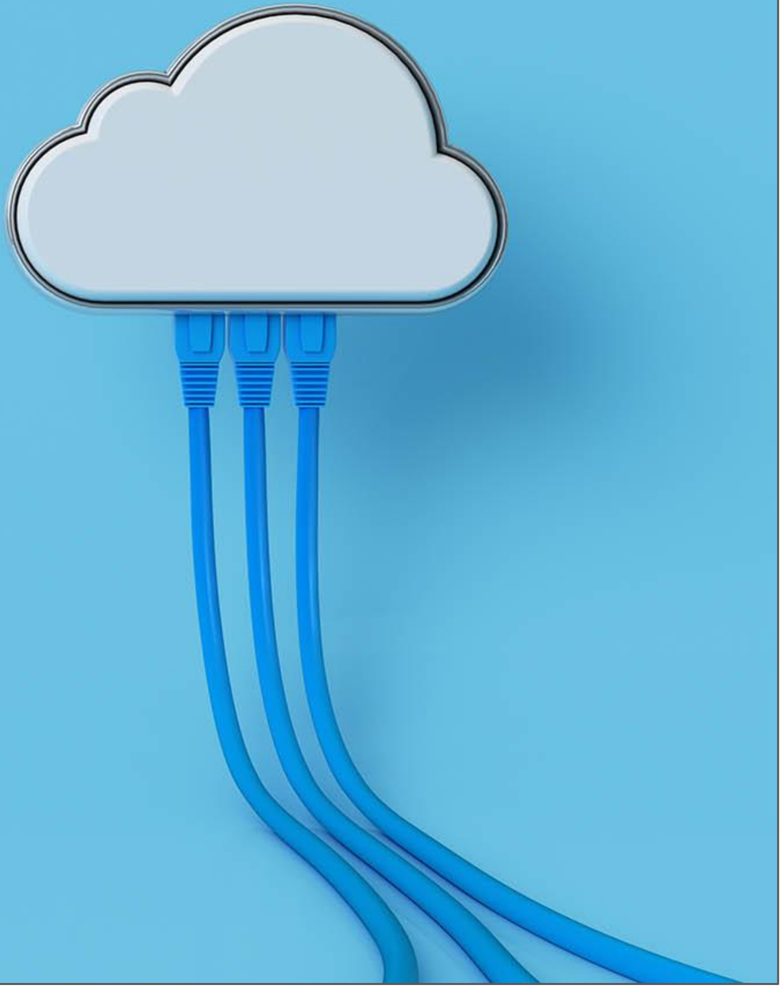
$3 MILLION

.25 FTE AND ~$10,000 FOR IT

More than 90% of nonprofit organizations are using cloud computing today

Half of them are using multiple cloud services

92% allow staff to access organizational data on personal devices



Which cloud services platform does your organization primarily use?

G Suite

Office 365

Box

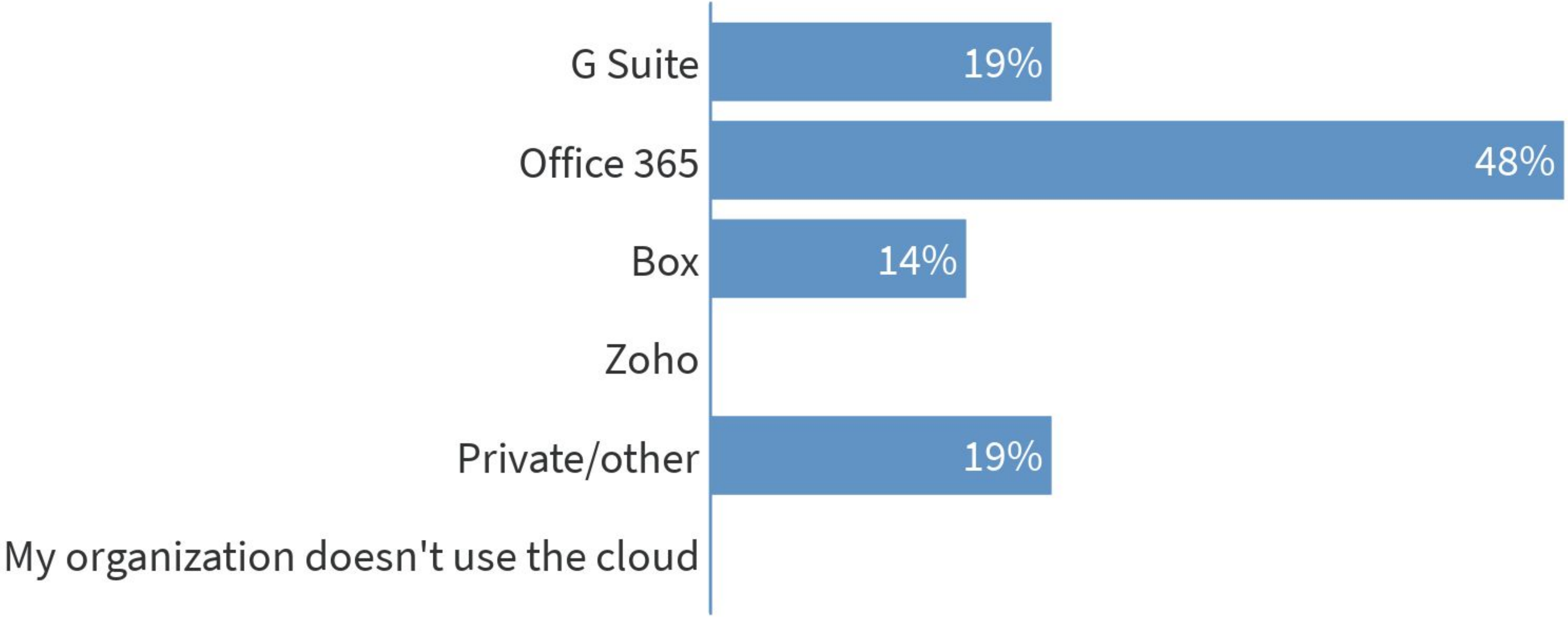
Zoho

Private/other

My organization doesn't use the cloud

When poll is active, respond at **PollEv.com/perryb188**

Which cloud services platform does your organization primarily use?



Poll Everywhere

1. Affordable, scalable
2. Secure, current
3. Efficient, reliable
4. Accessible

1. Sprawl
2. Control, oversight
3. Compliance
4. Security, privacy

OCEAN OUTCOMES

O2 Internet Technology Acceptable Use Policy

Table of Contents

Does your organization have a strong and vetted IT policy?

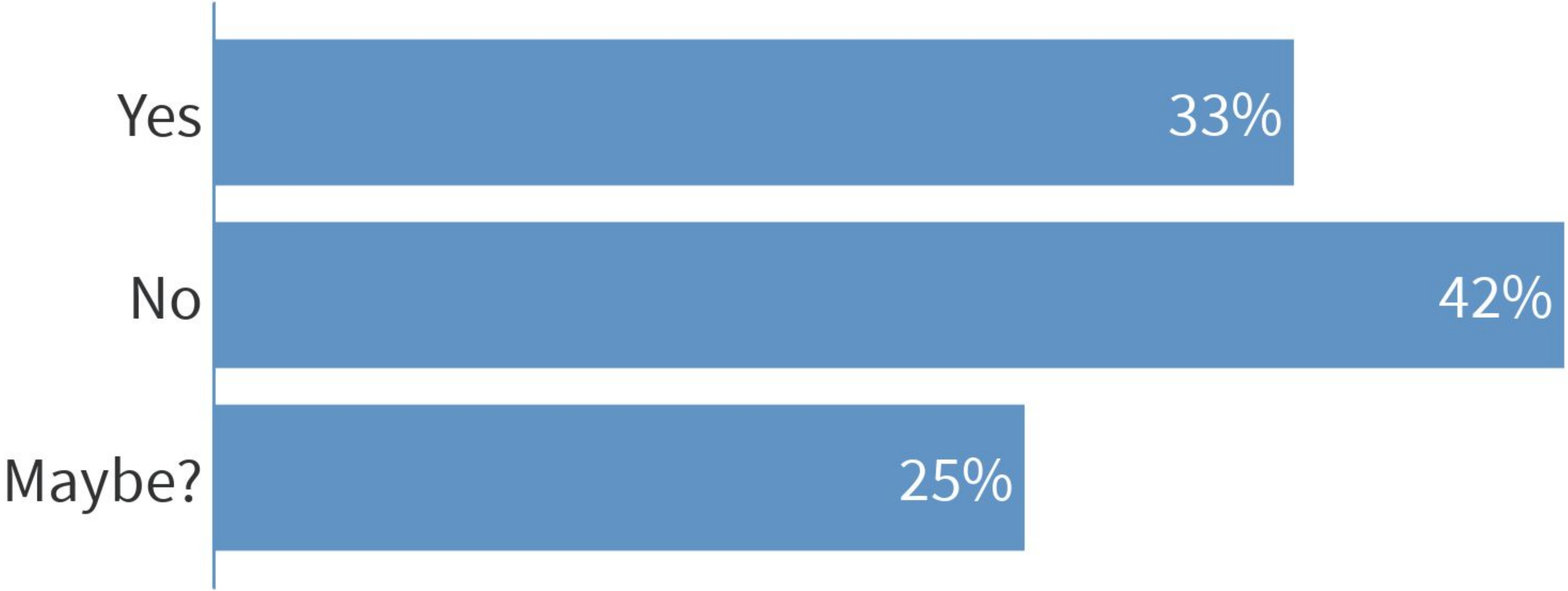
Yes

No

Maybe?

When poll is active, respond at **PollEv.com/perryb188**

Does your organization have a strong and vetted IT policy?



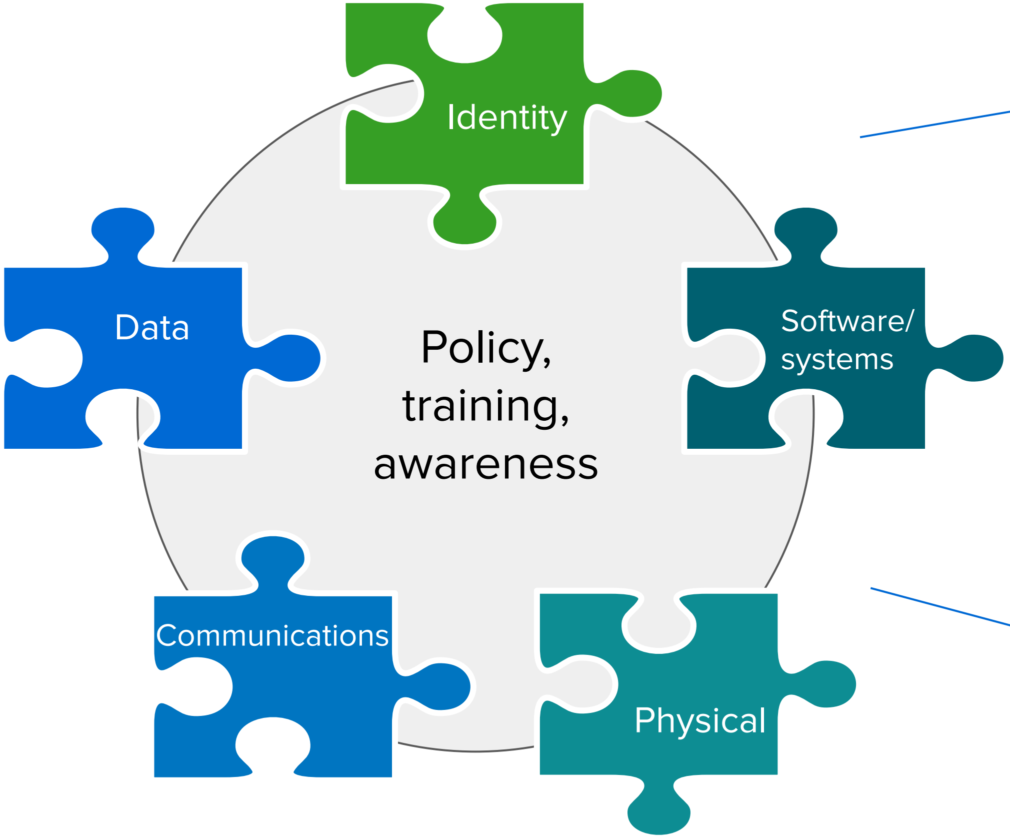
Poll Everywhere

OCEAN OUTCOMES

O2 Internet Technology Acceptable Use Policy

Table of Contents

SECURITY AREAS AND BEST PRACTICES



1. Security area overview and objective
2. Best practices at and/or for Ocean Outcomes
3. Audience poll

DATA SECURITY

Ensure data can’t be lost, aren’t intentionally or accidentally put somewhere unsafe, and aren’t exposed to untrusted or unwanted parties.

BEST PRACTICES

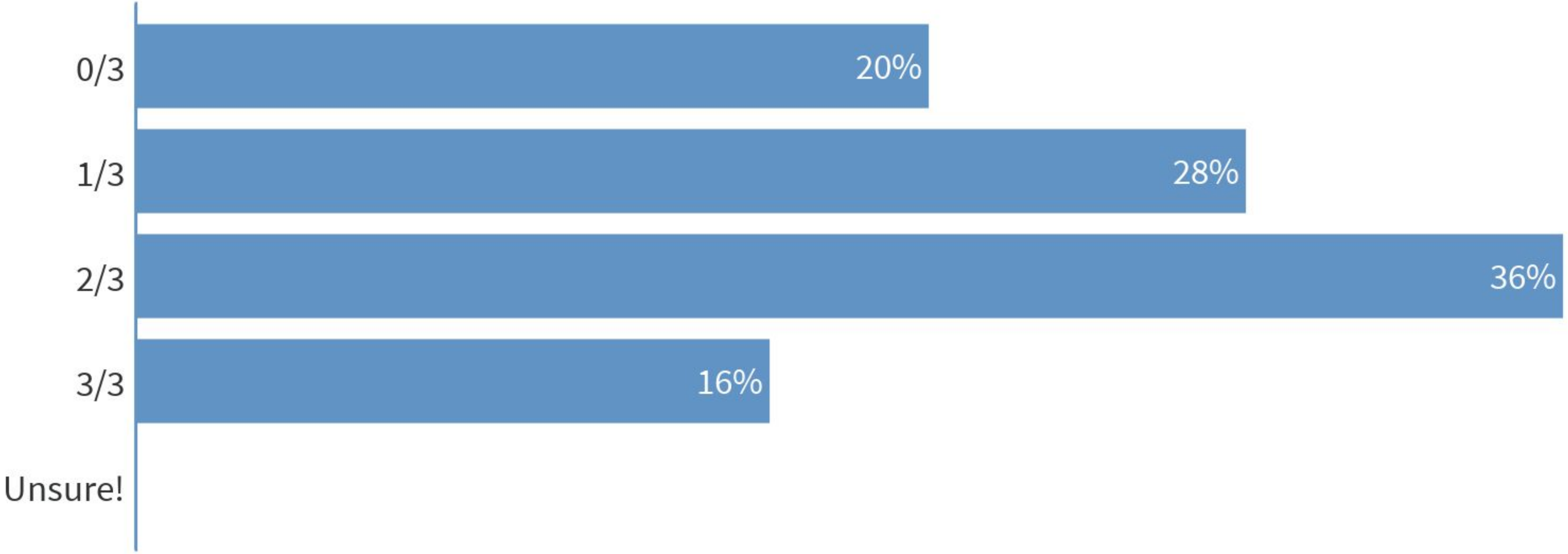
- Redundancy
  - ✓ Third-party backup
- Procedural documentation
  - ✓ Process templates
- Data loss prevention/monitoring
  - ✓ Permissions monitoring

How many of these data security best practices (redundancy, procedural documentation, and data loss prevention/monitoring) are in place at your organization?

Total Results: 0

ⓘ Poll is full and no longer accepting responses

How many of these data security best practices (redundancy, procedural documentation, and data loss prevention/monitoring) are in place at your organization?



Total Results: 25

Poll Everywhere

IDENTITY SECURITY

Ensure only the right people are access data and systems, and that it’s always possible to know who is accessing what.

BEST PRACTICES

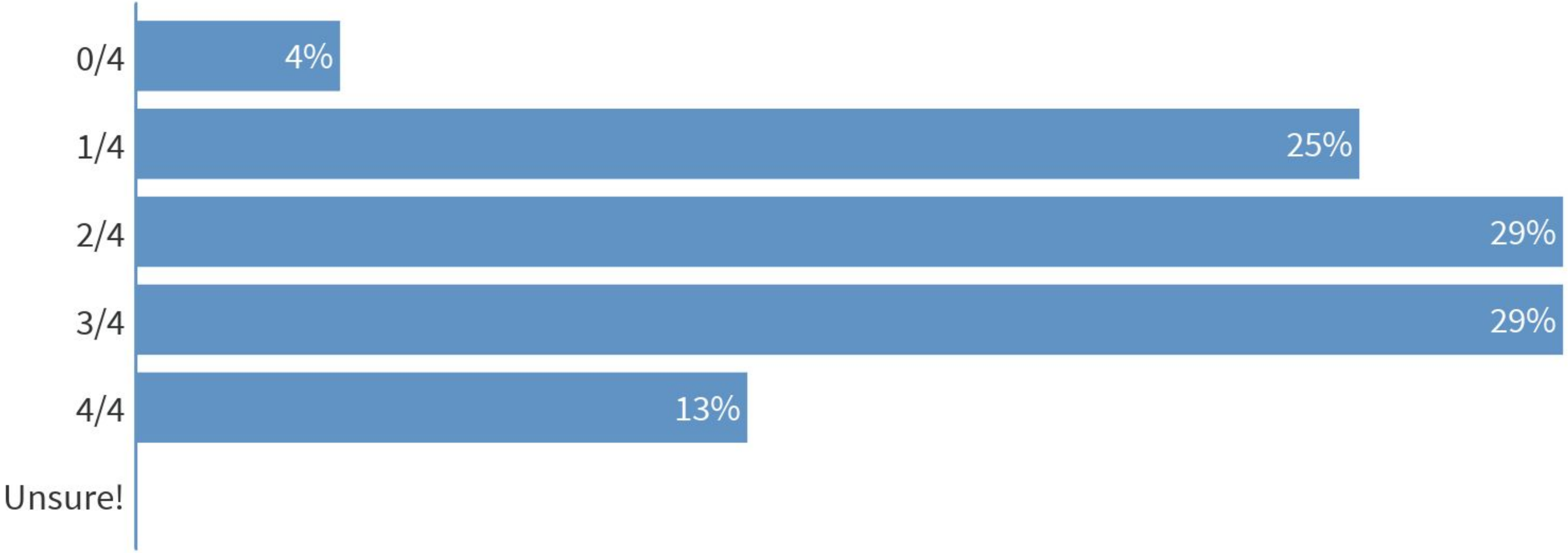
- User authentication
  - ✓ 2FA or MFA
- Password management
  - ✓ Password storing/sharing software
- Login alerts/monitoring
  - ⚠ …
- Succession plan
  - ⚠ …

How many of these identity security best practices (MFA, password manager, login alerts/monitoring, and succession plan) are in place at your organization?

Total Results: 0

When poll is active, respond at **PollEv.com/perryb188**

How many of these identity security best practices (MFA, password manager, login alerts/monitoring, and succession plan) are in place at your organization?



Total Results: 24

Poll Everywhere

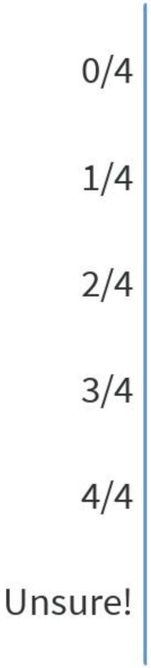
COMMUNICATIONS SECURITY

Protect data from being viewed or modified by untrusted parties and protect devices from external attacks.

BEST PRACTICES

- Firewall
  - ✓ Mandated, checked annually
- Virtual private network (VPN)
  - ✓ Mandated, configured at hire
- Website features
  - ⚠ ...
- DMARC and DKIM
  - ⚠ ...

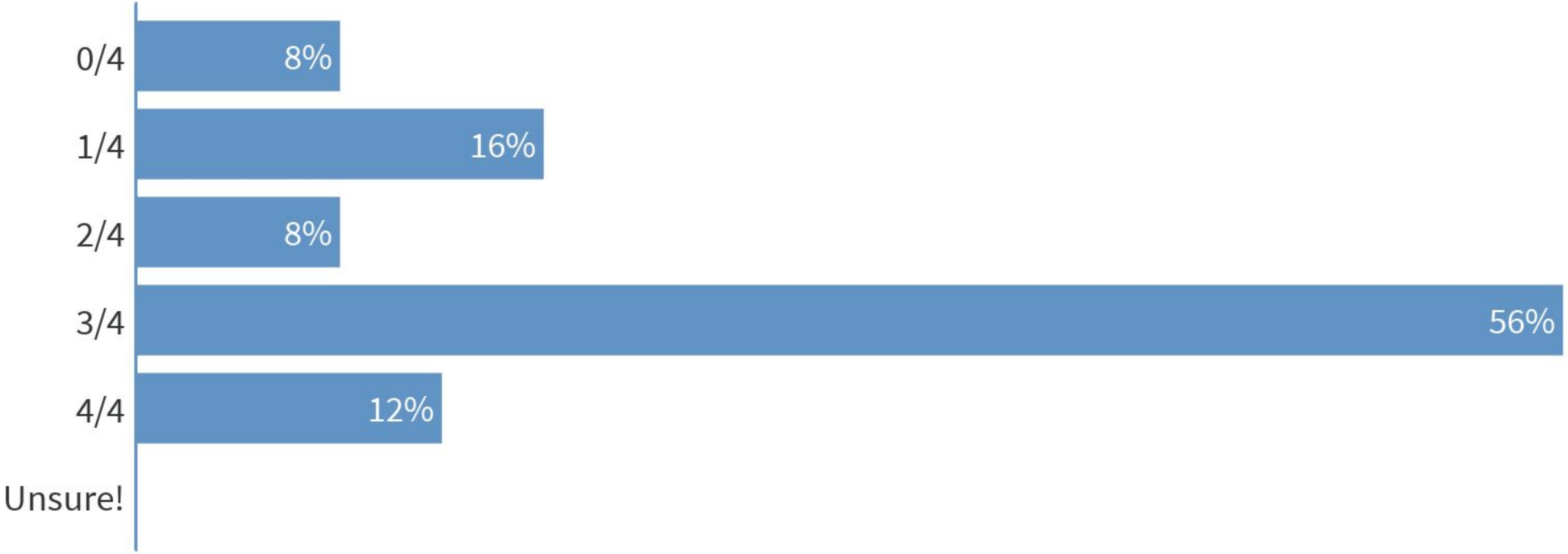
How many of these communications security best practices (firewall, VPN, website features, and DMARK and DKIM) are in place at your organization?



Total Results: 0

ⓘ Poll is full and no longer accepting responses

How many of these communications security best practices (firewall, VPN, website features, and DMARK and DKIM) are in place at your organization?



Total Results: 25

Poll Everywhere

SOFTWARE/SYSTEMS SECURITY

Maintain up-to-date software as first line of defense against exploits and malware, and to minimize risk when exposed to risky software, networks and websites.

BEST PRACTICES

- Software update requirements

  ✓ Mandated, checked annually

- Antivirus/malware

  ✓ Mandated, configured at hire

- Endpoint verification

  ⚠ ...

How many of these software/systems security best practices (software update requirements, antivirus/malware, and endpoint verification) are in place at your organization?

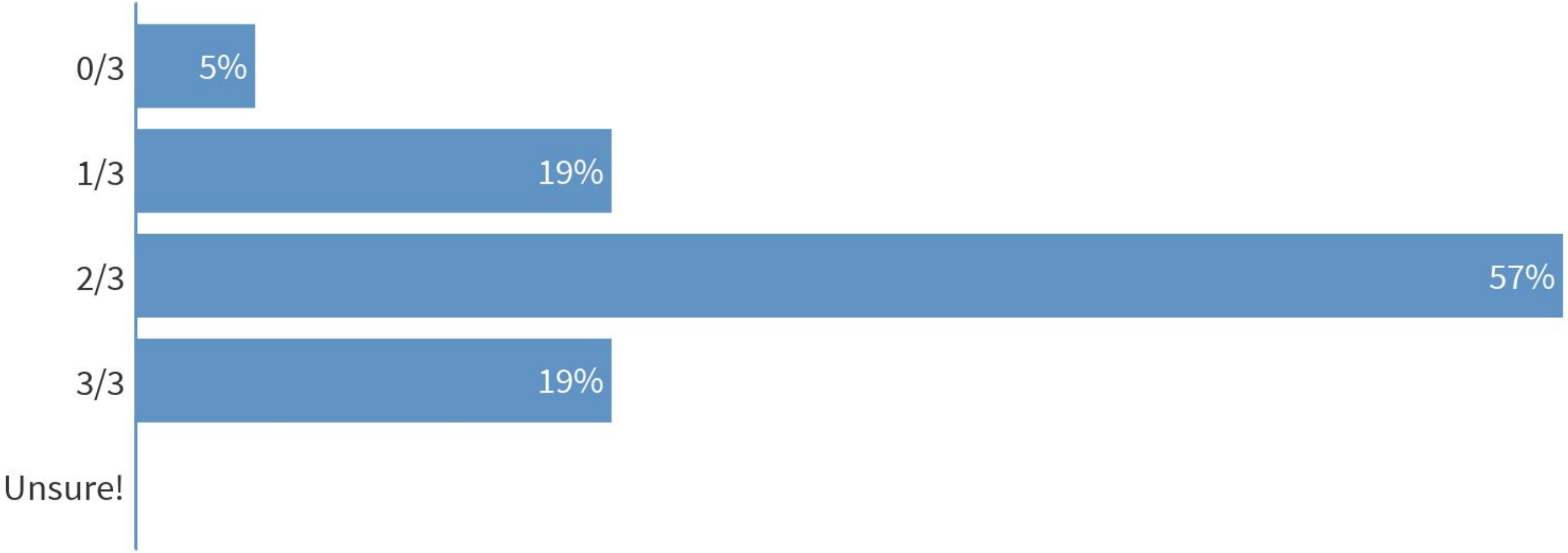
0/3
1/3
2/3
3/3
Unsure!

Total Results: 0

Start the presentation to see live content. Still no live content? Install the app or get help at **PollEv.com/app**

When poll is active, respond at **PollEv.com/perryb188**

How many of these software/systems security best practices (software update requirements, antivirus/malware, and endpoint verification) are in place at your organization?



Total Results: 21

PHYSICAL SECURITY

Keep devices safe and ensure that device loss or theft will not endanger the organization.

BEST PRACTICES

- Device encryption

  ⚠ ...

- Mobile device management

  ✓ Review, approval, requirements

- Features restrictions

  ⚠ ...

How many of these physical security best practices (device encryption, mobile device management, and features restrictions) are in place at your organization?

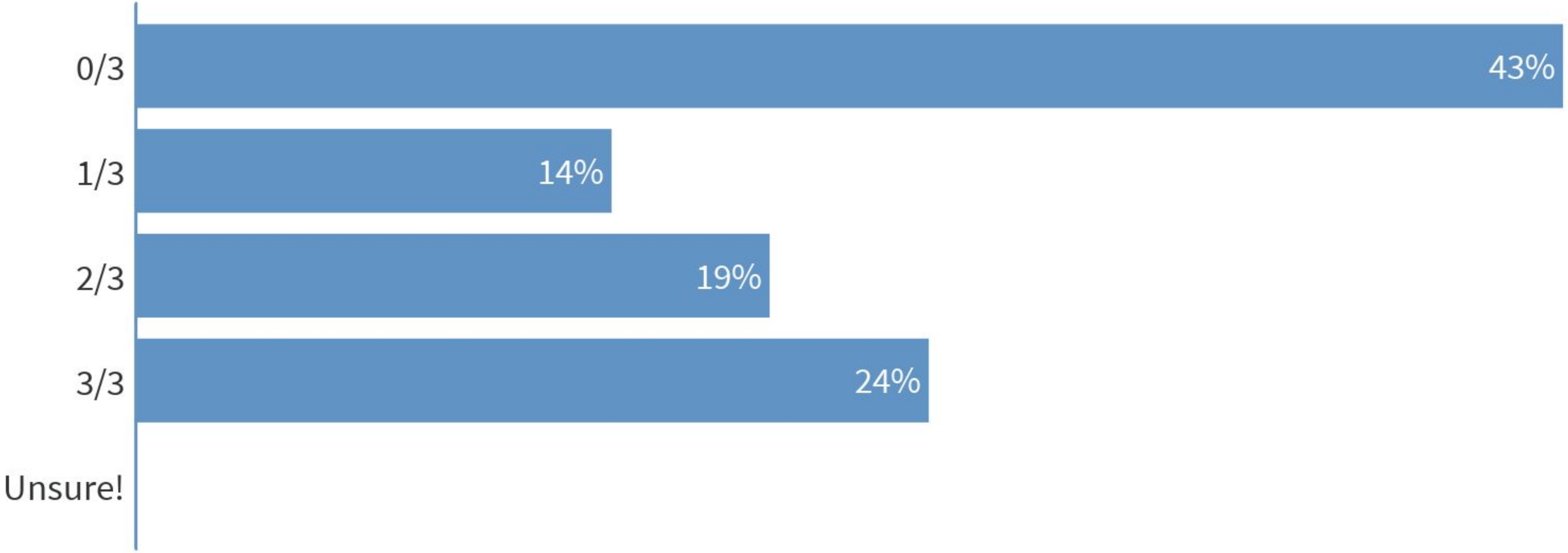
0/3
1/3
2/3
3/3
Unsure!

Total Results: 0

Start the presentation to see live content. Still no live content? Install the app or get help at **PollEv.com/app**

When poll is active, respond at **PollEv.com/perryb188**

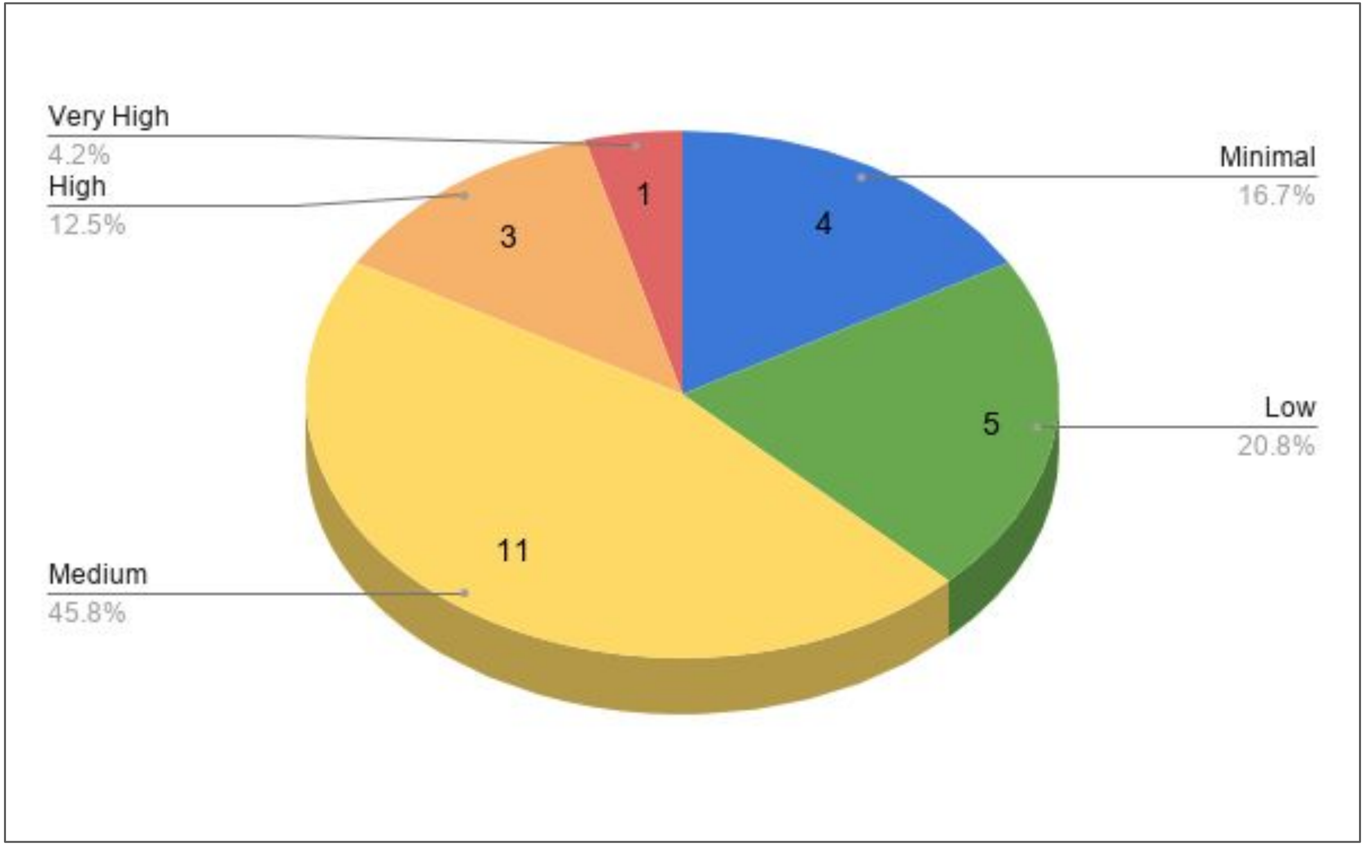
How many of these physical security best practices (device encryption, mobile device management, and features restrictions) are in place at your organization?



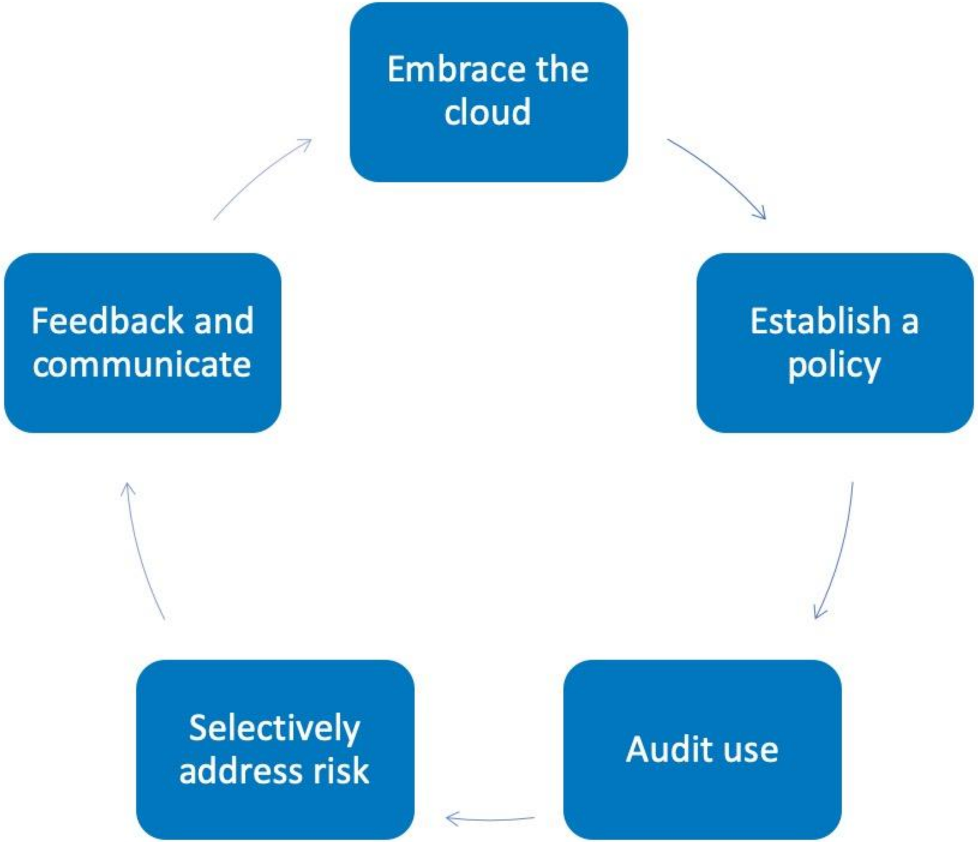
Total Results: 21

Poll Everywhere

OCEAN OUTCOMES RISK ACROSS ALL SECURITY AREAS



TAKEAWAYS


Embrace the cloud
Establish a policy
Audit use
Selectively address risk
Feedback and communicate