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

Perry Broderick
23 September 2019
Goals:

- Leverage O2 experience as a fully transparent case study
- Review of best practices in cloud services security
- Generate enthusiasm towards improving security

PollEv.com/perryb188

Agenda:

- Speak about O2
- Cloud services and nonprofits
- Best practices in cloud services use
How would you describe your organization's IT environment and its security?
How would you describe your organization's IT environment and its security?
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
Which cloud services platform does your organization primarily use?

- G Suite: 19%
- Office 365: 48%
- Box: 14%
- Zoho: 19%
- Private/other: 19%
- My organization doesn't use the cloud
1. Affordable, scalable
2. Secure, current
3. Efficient, reliable
4. Accessible
1. Sprawl
2. Control, oversight
3. Compliance
4. Security, privacy
O2 Internet Technology Acceptable Use Policy

Table of Contents

1. Purpose and Expectation
   1.1 Contractors, Partners, Interns, and Volunteers

2. Acceptable Use of Technology
   2.1 Prohibited Use

3. Technology Standards and Operating Environment
   3.1 Bring Your Own Device (BYOD)
      3.1.1 User Responsibilities
      3.1.2 BYOD Hardware and Software Requirements
   3.2 Internet Access
   3.3 Public WiFi and VPN Use

3. Individual Accounts
   3.3.1 Shared Accounts

3.4 Google Apps
   3.4.1 Google Drive
   3.4.2 Google Docs
   3.4.3 Google Calendar
   3.4.4 Google Chrome
   3.4.5 Google Contacts

3.6 Project Management and Internal Communication

6. Infrastructure Setup and Access
   6.1 Levels of Access and Systems Functionality

7. IT Services and Support
   7.1 Routine Maintenance
   7.2 Annual Audit

8. Acceptance and Agreement
Does your organization have a strong and vetted IT policy?

Yes

No

Maybe?
Does your organization have a strong and vetted IT policy?

- Yes: 33%
- No: 42%
- Maybe?: 25%
## O2 Internet Technology Acceptable Use Policy

### Table of Contents

1. Purpose and Expectation  
   1.1 Contractors, Partners, Interns, and Volunteers  
2. Acceptable Use of Technology  
3. Technology Standards and Operating Environment  
   3.1 Bring Your Own Device (BYOD)  
   3.1.1 User Responsibilities  
   3.1.2 BYOD Hardware and Software Requirements  
3.2 Internet Access  
   3.2.1 Public, Wi-Fi and VPN Use  
3.3 Individual Accounts  
   3.3.1 Shared Accounts  
3.4 Google Apps  
   3.4.1 Google Drive  
   3.4.2 Google Docs  
   3.4.3 Google Calendar  
   3.4.4 Google Chrome  
   3.4.5 Google Contacts  
3.5 Project Management and Internal Communication  
3.6 Other Telecommunications  
3.7 Software  
3.8 Accessing Accounts Through Third Party Apps  
4. Data Ownership  
5. Security and Disaster Recovery  
   5.1 Passwords and Account Security  
   5.1.1 Two Factor Authentication  
   5.1.2 Password Management Software  
   5.2 Hardware Security  
   5.3 Software Security  
   5.4 Data Backup and Recovery  
6. Infrastructure Setup and Access  
   6.1 Levels of Access and Systems Facility  
   6.2 Table of Infrastructure Assets, Access and Permission  
   6.3 External Infrastructure Access  
   6.4 Ensuring Responsibility Access Levels  
   6.5 Assigning, Editing, and Revoking Access  
   6.6 Confidential and Proprietary Information  
7. IT Services and Support  
   7.1 Routine Maintenance  
   7.2 Annual Audit  
8. Acceptance and Agreement
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?

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

Total Results: 0
How many of these data security best practices (redundancy, procedural documentation, and data loss prevention/monitoring) are in place at your organization?

- 0/3: 20%
- 1/3: 28%
- 2/3: 36%
- 3/3: 16%
- Unsure!
IDENTITY SECURITY

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

- 0/4: 4%
- 1/4: 25%
- 2/4: 29%
- 3/4: 29%
- 4/4: 13%

Total Results: 24
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?

- 0/4
- 1/4
- 2/4
- 3/4
- 4/4
- Unsure!

Total Results: 0
How many of these communications security best practices (firewall, VPN, website features, and DMARK and DKIM) are in place at your organization?

- 0/4: 8%
- 1/4: 16%
- 2/4: 8%
- 3/4: 56%
- 4/4: 12%

Total Results: 25
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?
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: 5%
- 1/3: 19%
- 2/3: 57%
- 3/3: 19%
- Unsure: 0%

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

- 0/3: 43%
- 1/3: 14%
- 2/3: 19%
- 3/3: 24%
- Unsure!
OCEAN OUTCOMES RISK ACROSS ALL SECURITY AREAS

- Very High: 4.2%
- High: 12.5%
- Minimal: 16.7%
- Low: 20.8%
- Medium: 45.8%
TAKEAWAYS

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