

Cyber-Security is dead. Long live Cyber-Resilience!

REDW_{LLC} expertise.

An epic journey across high mountains of techno-babble,
deep into jungles of arcane regulations,
through muddy swamps of politics,
across bleak deserts of funding.

This is my
mother-in-law,
Vivian



"Hi Vivian, this is
Apple Support.
Your computer has
a very serious
problem. But our
technicians can
help"



This is my
friend and
colleague,
Bryce Gibbs
CIO



"Please wire the
\$60k payment
on the property
before
tomorrow's
closing"



YOUR BEST CHOICE!

Family, friends,
co-workers -
every one of us
is a target to be
exploited.





The Internet has
unleashed a dark
side along with
all of the cool
stuff like
Facebook

Cyber-Risk = Business Risk

- Hacked? = Business Interruption
- Breached? = Reputational Loss, Liability Claims
- Non-Compliant? = Fines & legal action

'Cyber-Risk' means any risk of financial loss, disruption, or damage to the reputation of an organization from some sort of failure of its information technology systems

Institute of Risk Management, 2014

1. Your organization gets hacked and you suffer a reportable (public) **data breach**
2. An employee opens a phishing email and infects the whole network and **your operations come to a halt**
3. You open an email and infect your machine with Ransomware that **encrypts your AP, AR and GL files** - you have to pay the ransom in Bitcoin, but you can't get it setup in time. You lose your records and then your backup doesn't restore.
4. Your organization becomes collateral damage in a DDOS attack targeting another of your ISPs customers. Your access to **the Internet is effectively shut down**
5. You get a huge bill for a medical procedure you didn't have because **your medical records were breached**

6. You receive what appears to be legitimate instructions from an established vendor to wire payment to a different bank account. **The money is gone** by the time the vendor tells you they didn't receive the funds.
7. The disk storage array in your finance server fails – then you realize that the backups were never setup.
8. A payroll employee opens a phishing email that instructs her to change her password at bank. She gives away her credentials and **the payroll account is drained in 10 mins**
9. Your **credit cards stop working** because 'you' reported them lost and the replacement have been mailed to someone in another state
10. Your **IRS tax refund isn't coming** - it was paid to someone else

Data Breach Costs:

- \$ Reputation damage
- \$ Litigation defense
- \$ Forensic and clean up costs
- \$ Regulatory fines
- \$ Credit monitoring for those affected
- \$ Remedial technology

- \$2.14 million to HHS Office of Civil Rights (OCR)
- \$17 million in investments in security technology
- \$7.5 million to a fund to reimburse affected individuals
- \$7.45 million in attorneys' fees
- \$15,000 to the patient that found the data online

\$34,105,000



Over 90% of all
data breaches
result from
human error



"Amateurs
hack systems.
Professionals
hack people"

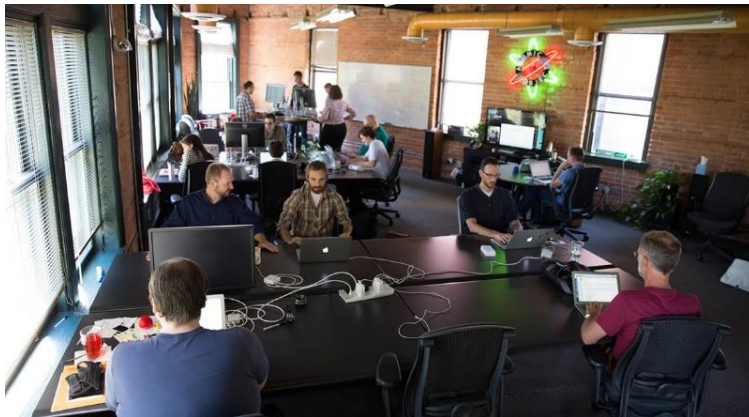
Bruce Schneier

Old

Data: On Premise

Computers: On Premise

Perimeter: Local Internet Connection



New

Data: Cloud

Computers: Anywhere

Perimeter: Everywhere



REDW LLC And we no longer have physical control our firewall...

Old

Firewall: Digital Gateway



New

Firewall: People



Yes, he's our new firewall. seriously...

REDW_{LLC} Our people are now our real firewall

This is the human
firewall we'd like to
think we have



REDW^{LLC} Our people are our real firewall

But this is more
like the human
firewall we really
have



Old

Prevention



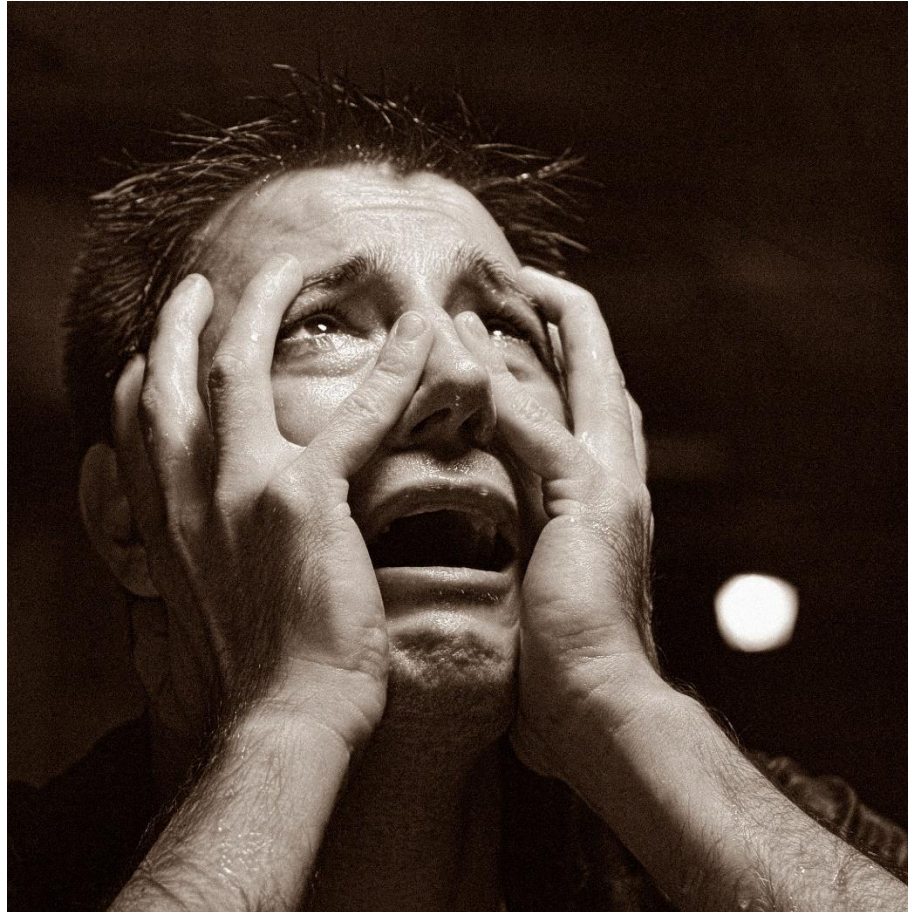
New

Resilience



Yes, him again...

REDW_{LLC} Yes, we are totally *#\$@ed.



CyberHealth

Our ability and willingness to protect ourselves and others from imminent harm, and stay safe from those who would exploit our families and community.



CyberHealth

1. Awareness
2. Clarity
3. Education
4. Hygiene
5. Assessment
6. Response
7. Recovery



CyberHealth is
no longer a
technology issue

Now it's a
cultural &
behavioral issue

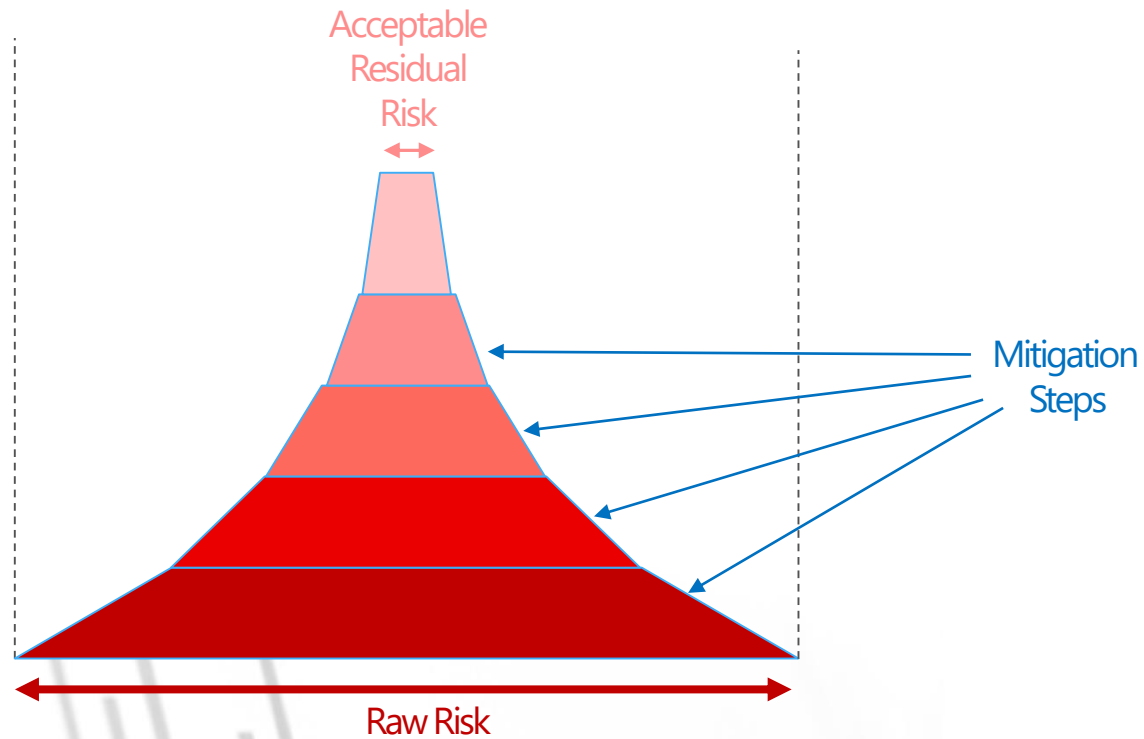


REDW LLC ... that can result in costly, life-sucking litigation

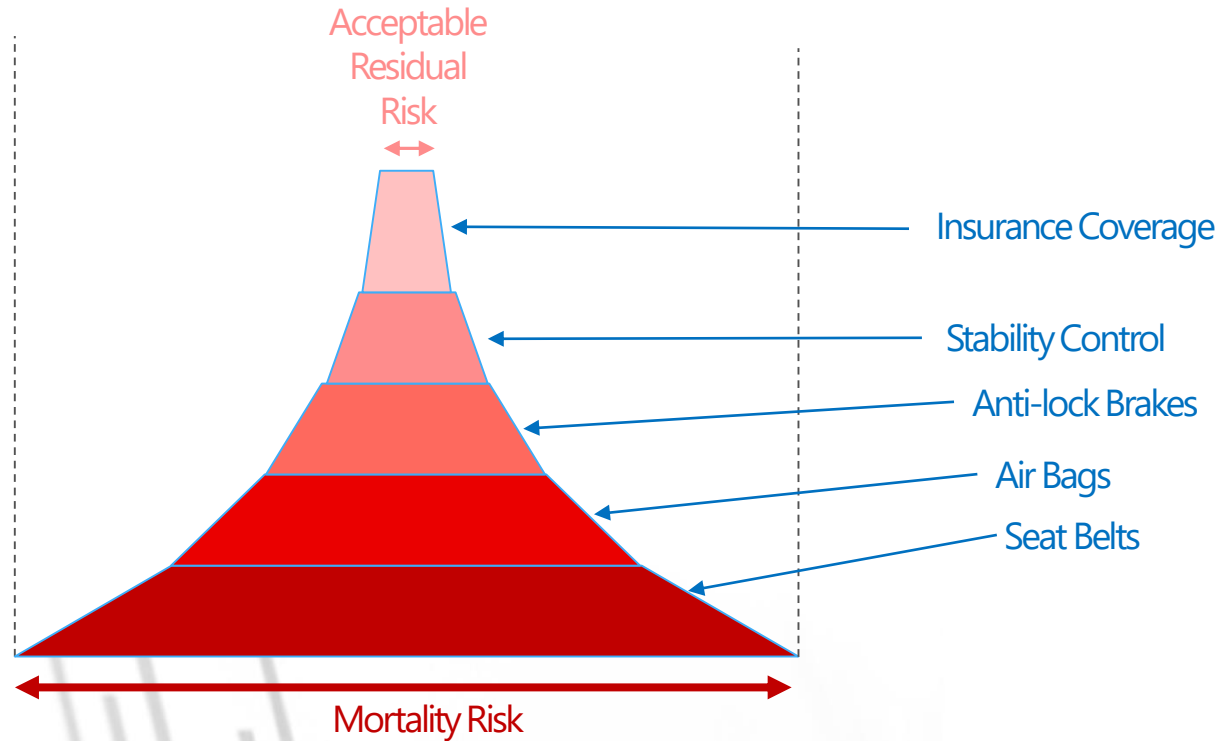
Unless an
afternoon of being
cross-examined is
your idea of fun.



Managing Exposure by Mitigation



Mitigating Auto Safety Exposure



IT Governance Review

- How have IT strategy and planning been formulated?
- What regulatory requirements are applicable?
- Who is responsible for executing IT strategy?
- Is all software licensed and documented?

Governance & Compliance

Policy & Procedure Review

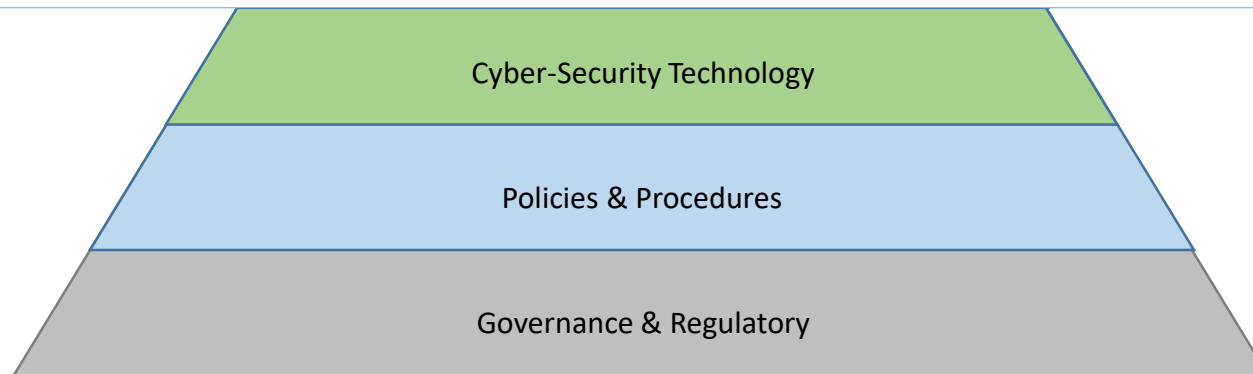
- Inventory and evaluate current policies and procedures

Policies & Procedures

Governance & Compliance

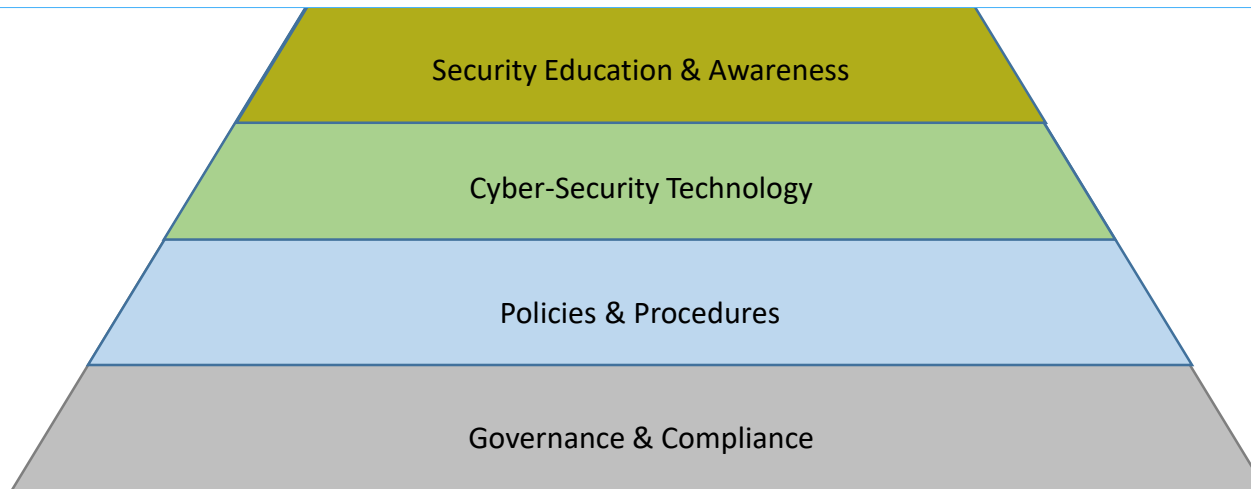
Cyber-Technology Review

- Assess overall security technology & architecture



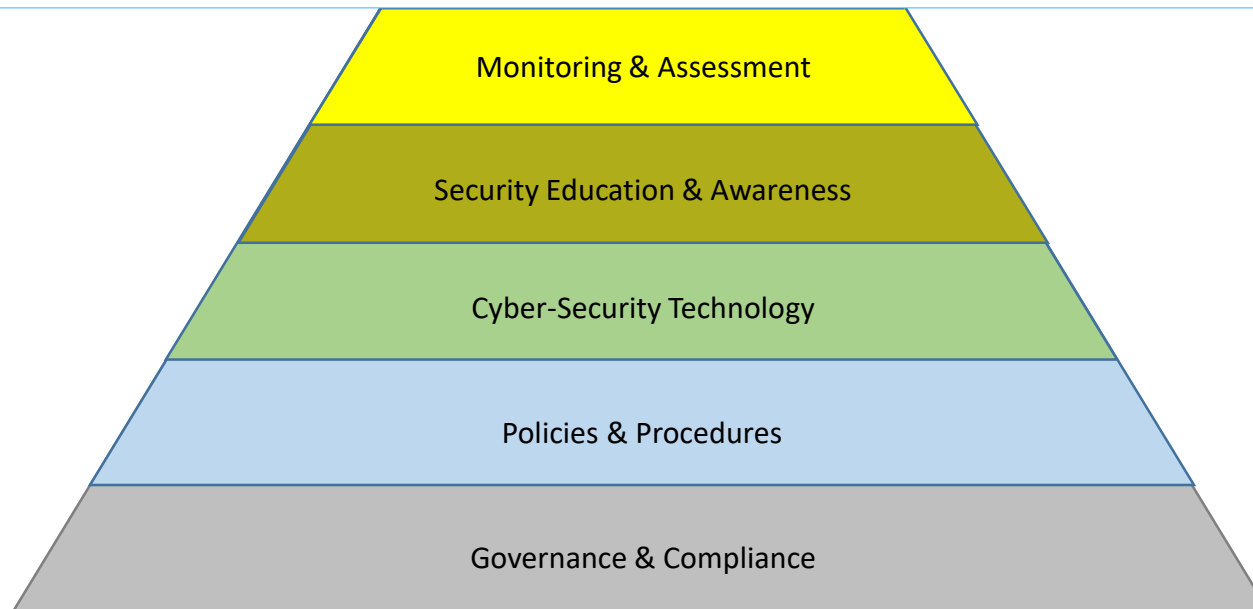
Security Education & Awareness Review

- Assess current & past security education & awareness efforts
- Identify regulatory requirements for security education & awareness



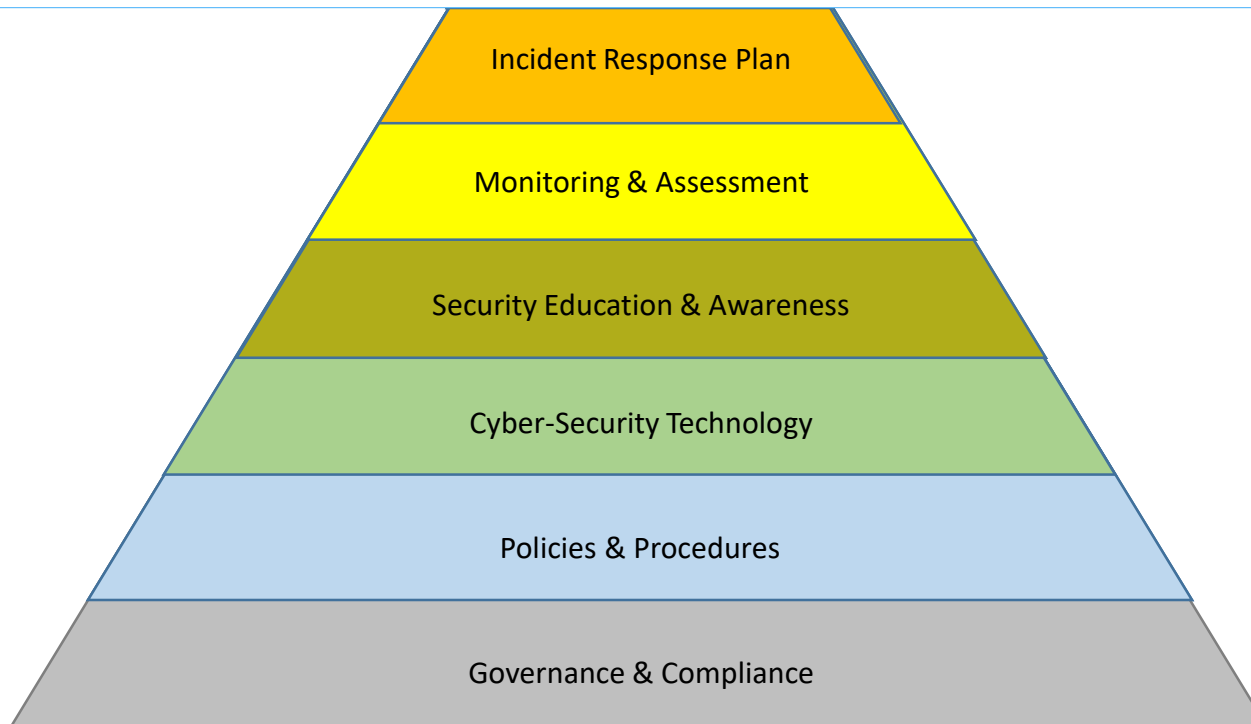
Monitoring & Assessment Review

- Assess existing monitoring systems
- Assess existing assessment methods of technology systems
- Assess existing assessment methods of employee behavior



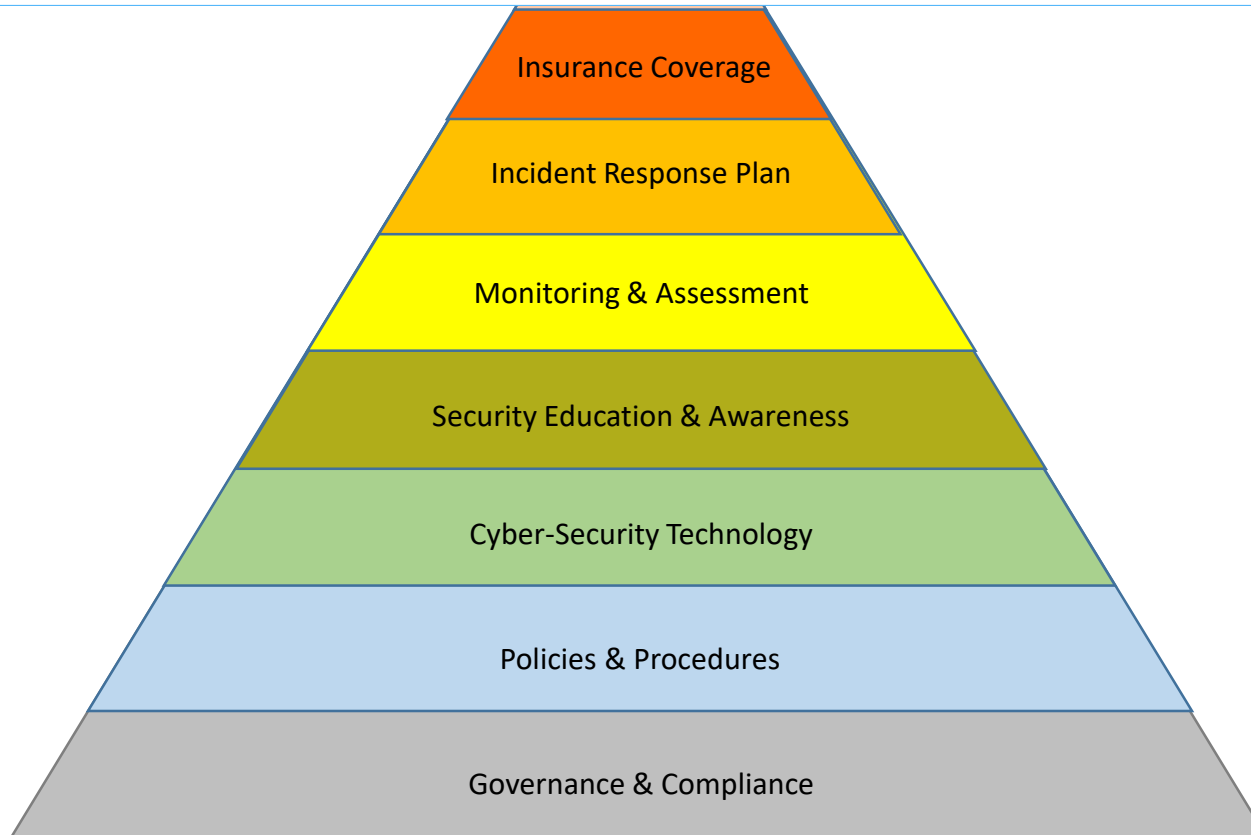
Incident Response

- Assess existing incident response policy & documentation



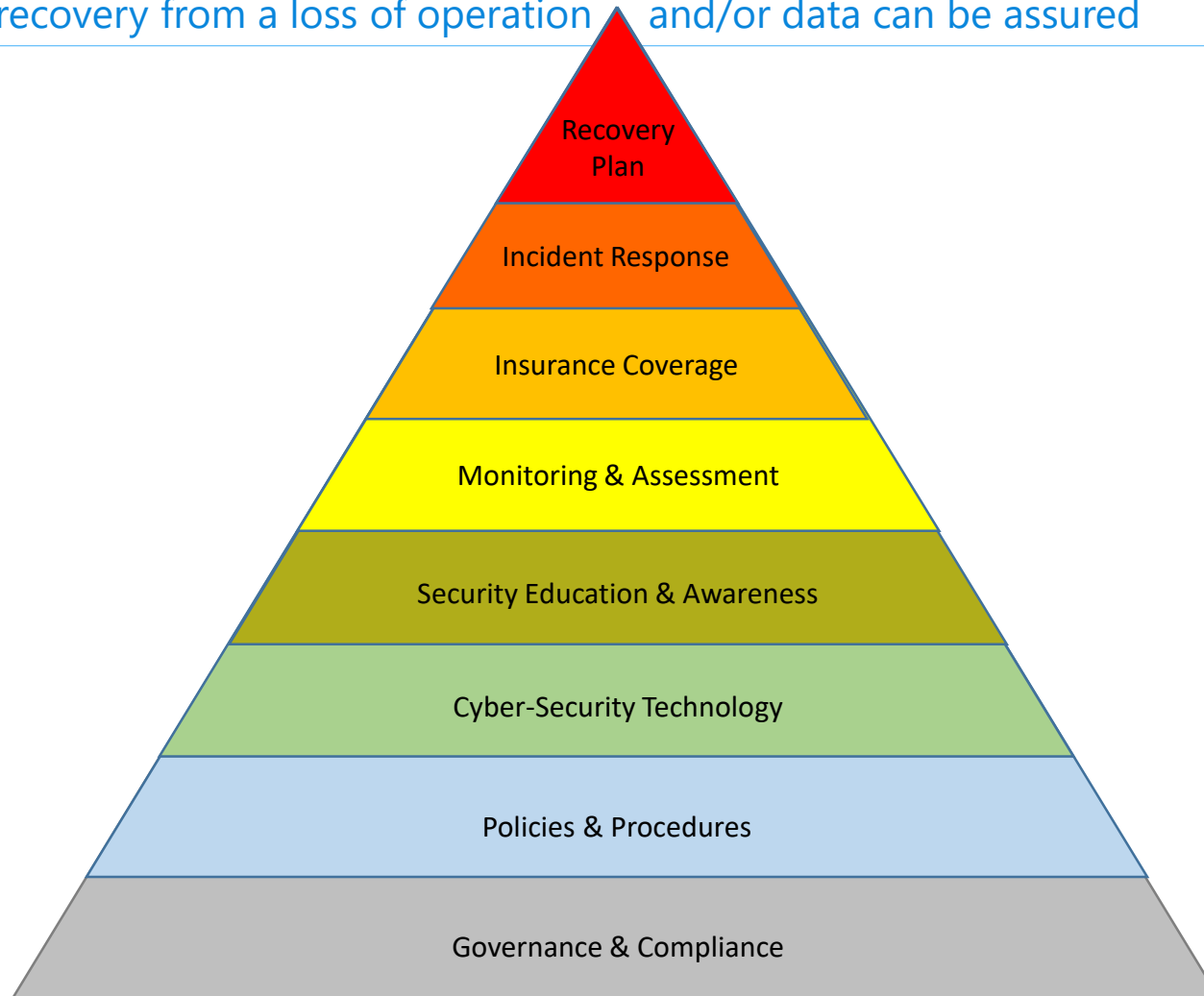
Insurance Review

- Evaluate current coverage of existing policies

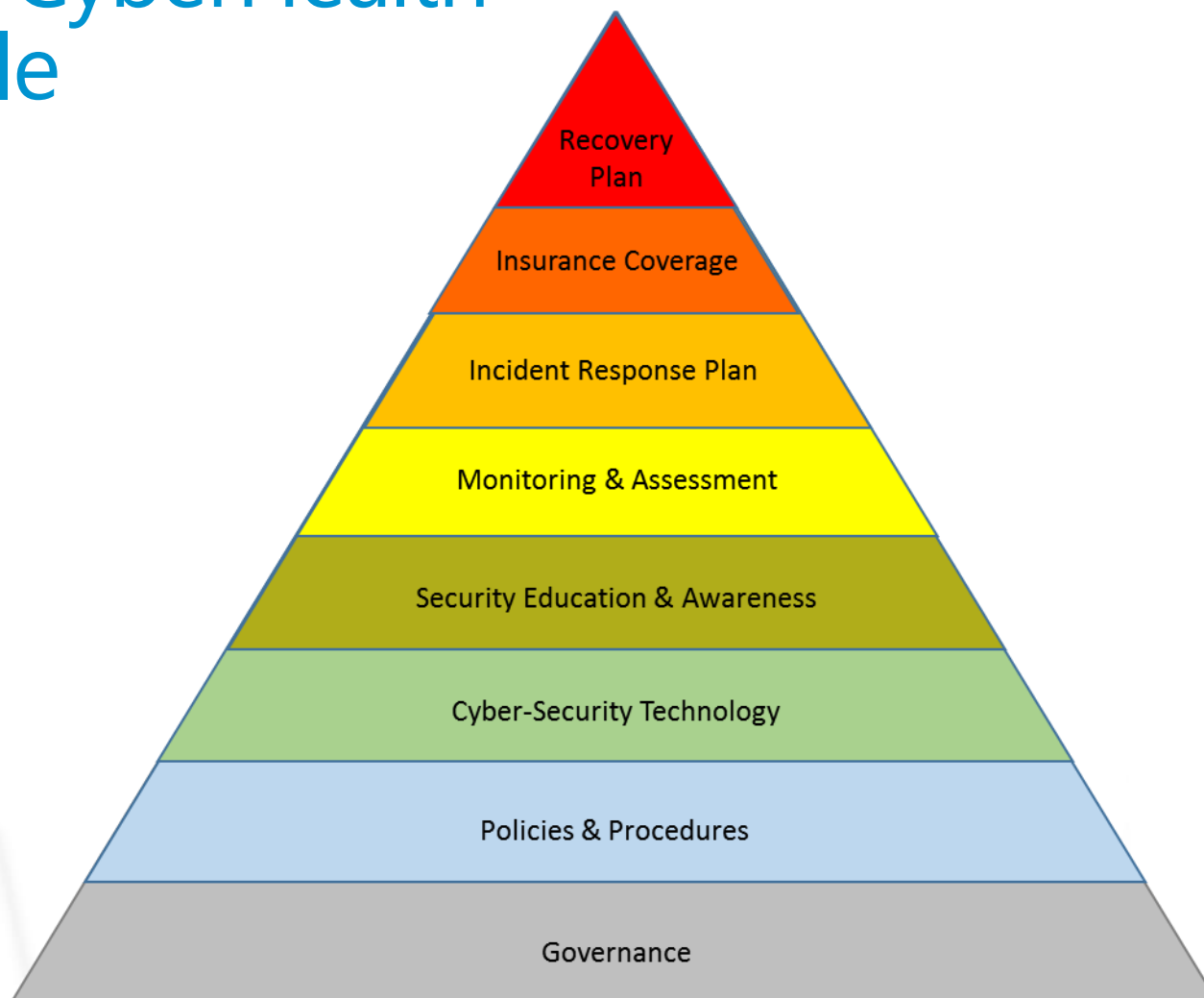


Recovery:

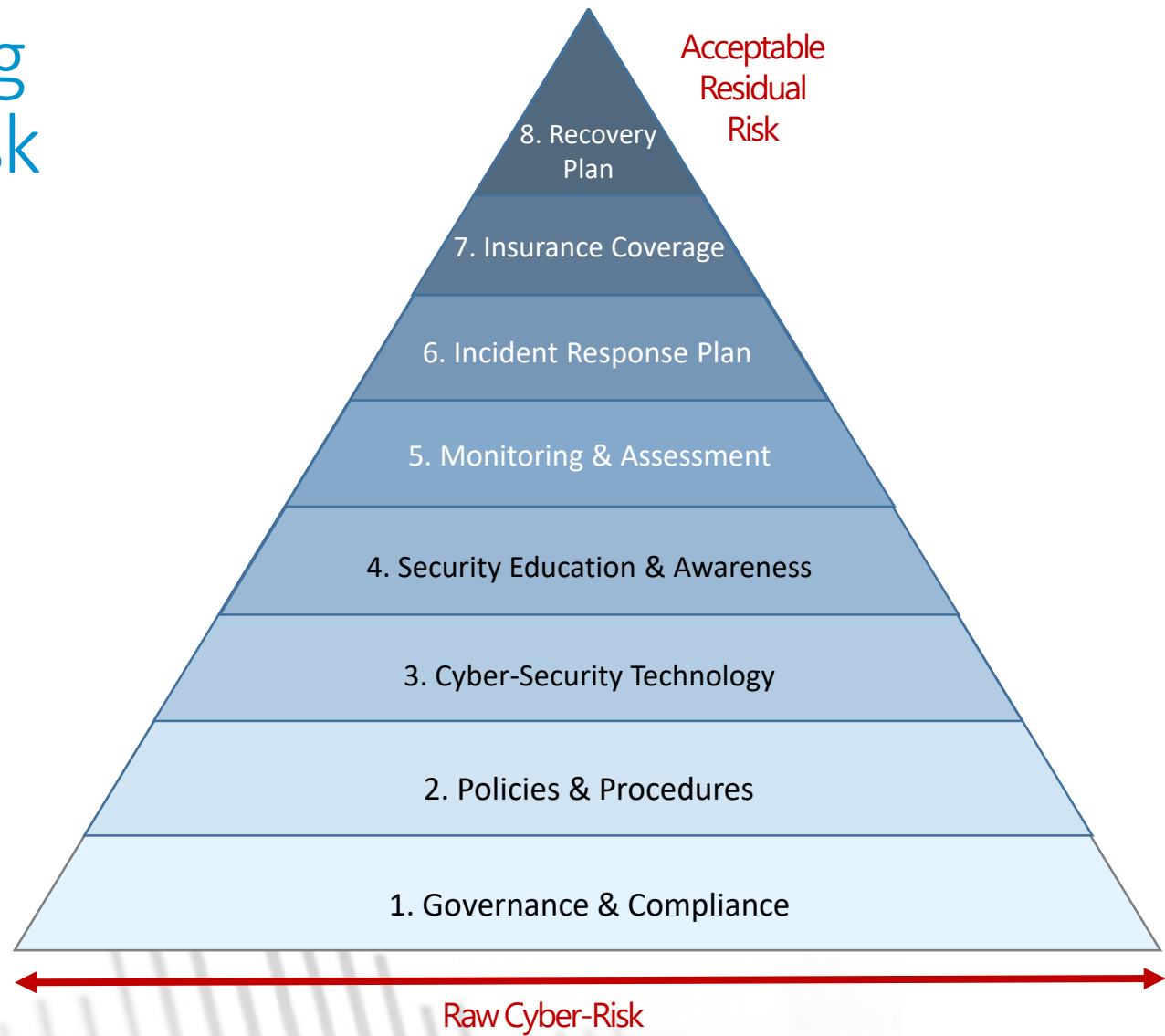
- The DR/BC Plan needs to be tested at least annually to ensure that recovery from a loss of operation and/or data can be assured



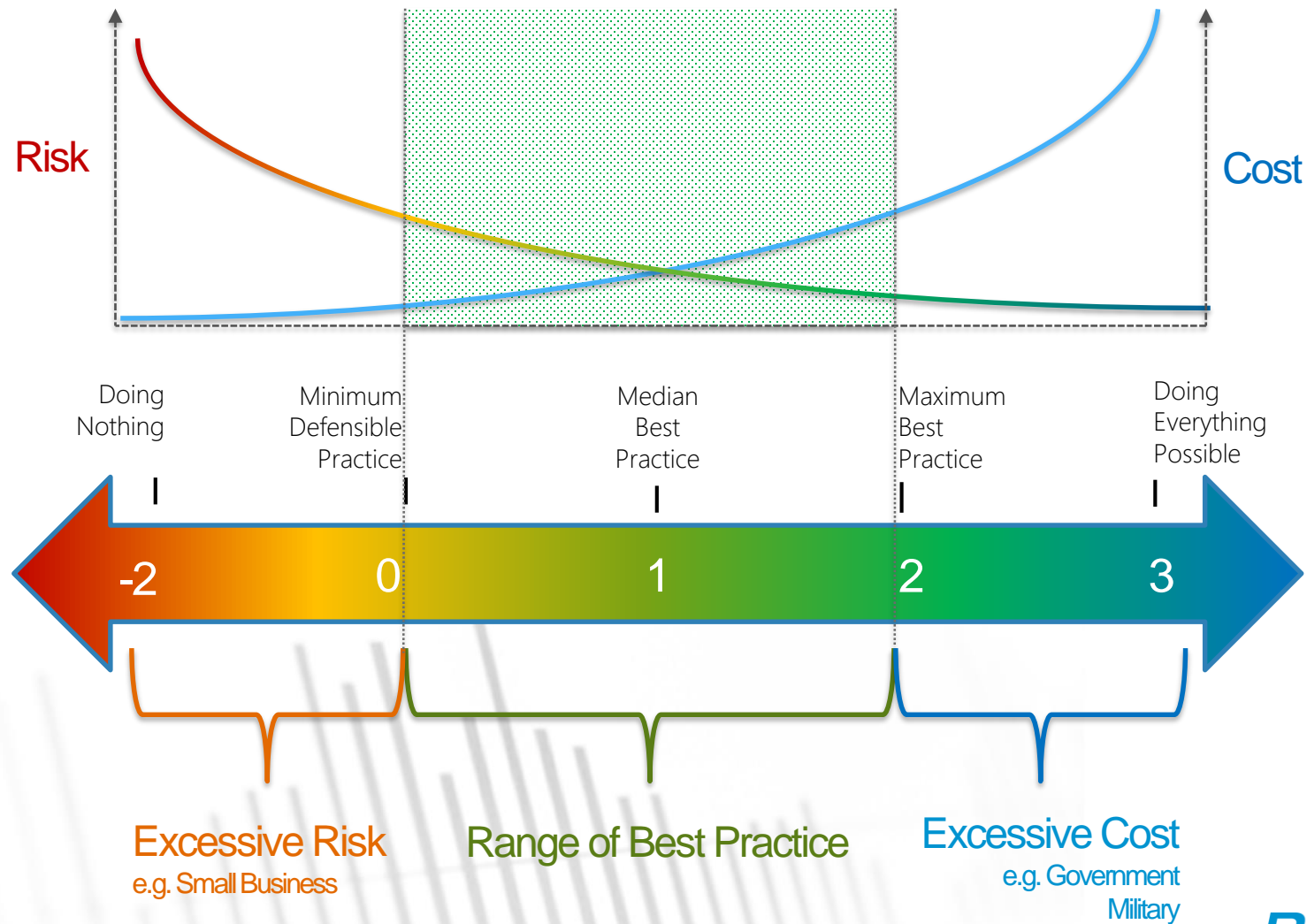
Your CyberHealth Profile



Mitigating Cyber-Risk

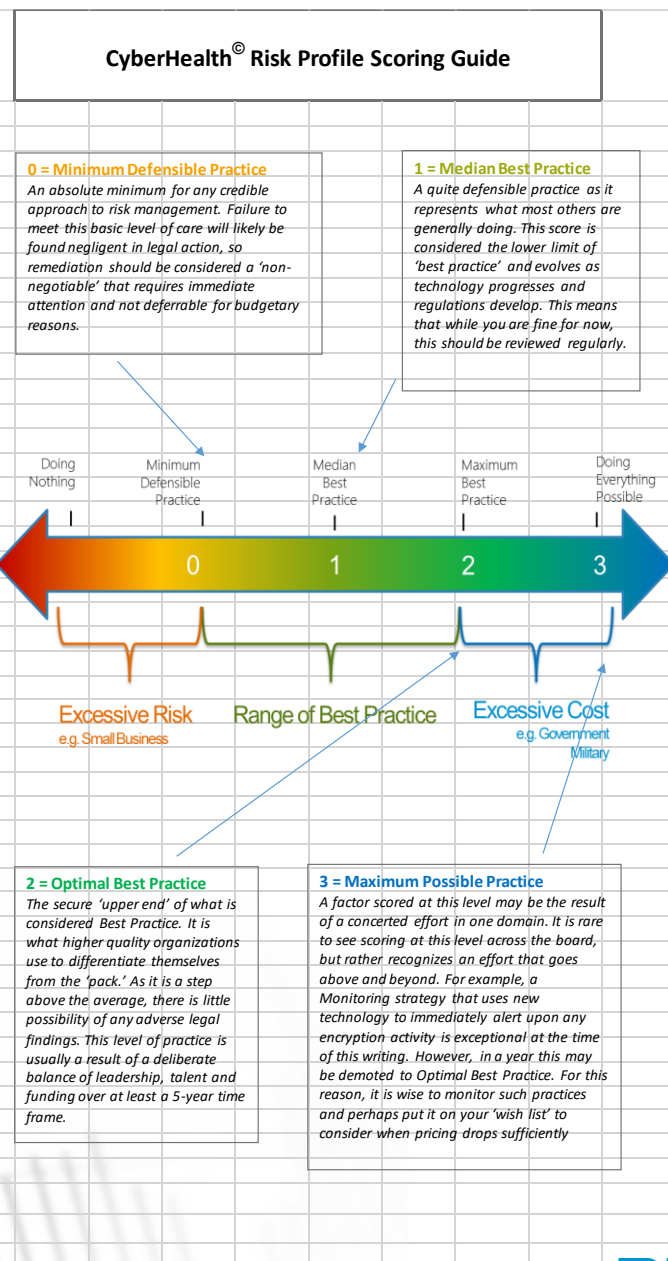


Balancing Risk vs. Cost



1. Peer-reviewed cyber-security journals
2. Court rulings on cyber-security litigation
3. Capabilities & costs of emergent technology
4. Networks of security professionals
5. Conferences, meetings, papers & posts
6. Location, size and type of organization
7. Regulatory compliance requirements

| CyberHealth Rapid Review Estimate | | Risk Factor Average | Risk Factor Coverage |
|-----------------------------------|---|---------------------|----------------------|
| 1 | Governance | 0.3 | 52% |
| 1.1 | Governance | 0.8 | 71% |
| 1.2 | Process | -0.3 | 33% |
| 2 | Policies & Procedures | 0.4 | 44% |
| 2.1 | Plans | 0.0 | 56% |
| 2.2 | Policies | 0.3 | 32% |
| 2.3 | Procedures | 0.1 | 6% |
| 2.4 | Documentation | 1.0 | 100% |
| 3 | Cybersecurity Technology | 0.5 | 58% |
| 3.1 | Firewall | 1.4 | 100% |
| 3.2 | Email Security | 1.1 | 80% |
| 3.3 | Endpoint Security | 0.3 | 25% |
| 3.4 | Access Control | 0.6 | 44% |
| 3.5 | Mobile/Encryption | -1.0 | 40% |
| 4 | Security Education & Awareness | -0.7 | 7% |
| 4.1 | Administration | -1.2 | 0% |
| 4.2 | Onboarding | 0.0 | 20% |
| 4.3 | Ongoing (Maintenance) | -0.8 | 0% |
| 5 | Monitoring & Assessment | 0.8 | 48% |
| 5.1 | Monitoring of Critical Infrastructure | 1.3 | 67% |
| 5.2 | Monitoring of Security Events | 0.8 | 55% |
| 5.3 | Assessment | 0.4 | 22% |
| 6 | Incident Response | 1.1 | 77% |
| 6.1 | Planning | 0.8 | 43% |
| 6.2 | Response Process | 1.0 | 100% |
| 6.3 | Investigative Process | 0.9 | 64% |
| 6.4 | Resources | 1.8 | 100% |
| 7 | Insurance Coverage | 1.8 | 100% |
| 7.1 | Planning | 1.5 | 100% |
| 7.2 | First Party Coverage | 2.0 | 100% |
| 7.3 | Third Party Coverage | 2.0 | 100% |
| 8 | Recovery | 0.7 | 80% |
| 8.1 | Planning | 1.3 | 100% |
| 8.2 | Data Protection | 0.9 | 75% |
| 8.3 | Data Recovery | 0.0 | 66% |
| Overall Estimated Score | | 0.6 | |
| Overall Factor Coverage | | | 58% |





How do we achieve resilience?

1. Our data
2. Our people
3. Our response
4. Our exposure



1. our data

Data, data, mountains of data



1. Data storage became dirt cheap
2. It wasn't worth our time to clean up
3. We end up with insane amounts of data
4. If that data contains PII or PHI, it's radioactive
5. Any data you possess is discoverable by law
6. Ignorance is no excuse.



1. Inventory ALL the data you have
2. Decide what data you really need to do business and legally retain.
3. Develop a comprehensive Data Retention & Destruction Policy, and create a plan to get compliant within 12 months.
4. Hunt down data that's 'out of policy' and purge it from storage and backup tapes.



REDW_{LLC} 2. our exposure

1. Forensic investigations
2. Consumer breach notification
3. Credit monitoring
4. PR/Crisis communications
5. Legal defense fees
6. Legal settlement costs
7. Crisis management



1. Operational disruption
2. Recovery costs
3. Regulatory compliance fines
4. Cybersecurity improvements
5. Devaluation of trade name
6. Increased cost to raise debt
7. Lost value of customer relationships
8. Loss of intellectual property





REDW^{LLC} insurance is a no-brainer for most organizations.

Most Cyber Liability Insurance offers coverage for:

- Forensics
- PR
- Legal
- Credit Monitoring
- Business Interruption & Recovery
- Breach Coordination service



3. our response

- data breach
- ransomware attack
- systems down

when trouble happens...



... you need responders who know what to do

1. Identify the people who you can count on in a crisis
2. An up-to-date written, and familiar plan,
3. Practice the process and refine the plan
4. Compliance with applicable regulations
5. Practice, practice, practice & document
6. Speed is critical – control the flow of information
7. Performance should exceed that of your peers'



4. our people

- employees
- contractors
- business associates

REDW_{LLC} we are so easily hooked...





REDW LLC ...or infect our computers with ransomware.



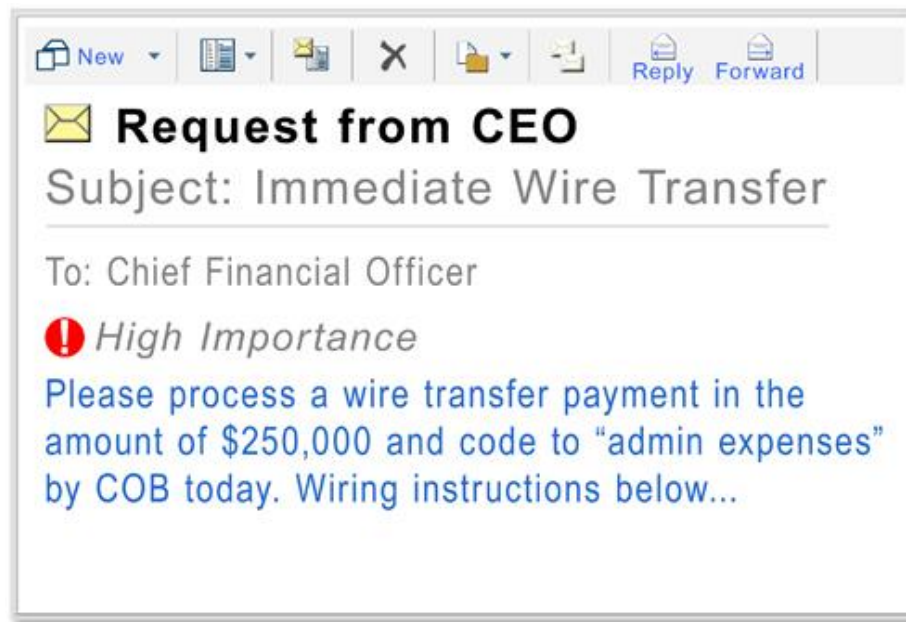
WARNING!

Your personal files are encrypted!

11:58:26

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open <http://maktubuyatq4rfyo.onion.link>
or <http://maktubuyatq4rfyo.torstorm.org>
or <http://maktubuyatq4rfyo.tor2web.org>





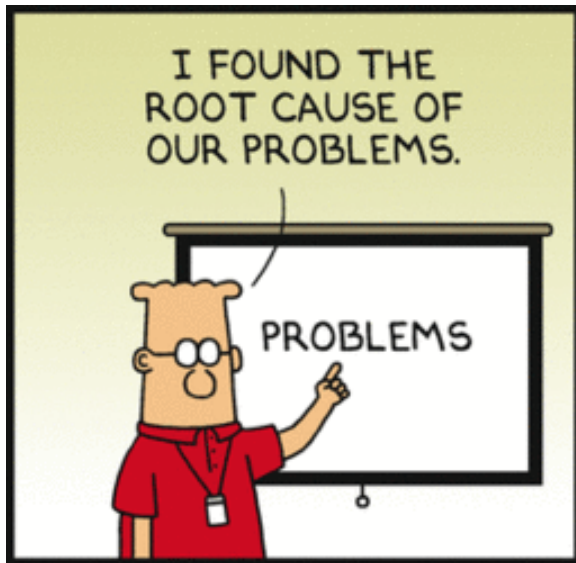
Security Awareness Education for Your Team

“In theory, one can build provably secure systems.
In theory, theory can be applied to practice
but in practice, it can't”

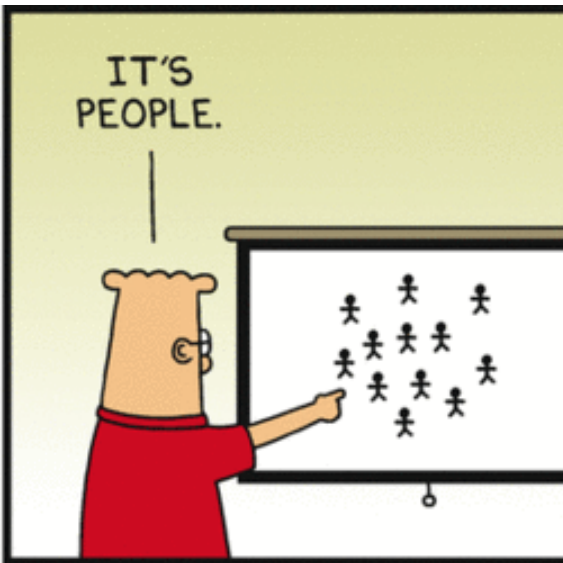
M. Dacier, Eurecom Institute

1. One hour live 'Security Awareness Training' every 1 or 2 years. 1 hour of CPE, but no assessment or follow-up training
2. New hires required to watch a video of the most recent training during their first week.
3. Agency 'temps' have no formal training
4. Independent Contractors sign a NDA and a BAA, but receive no training.

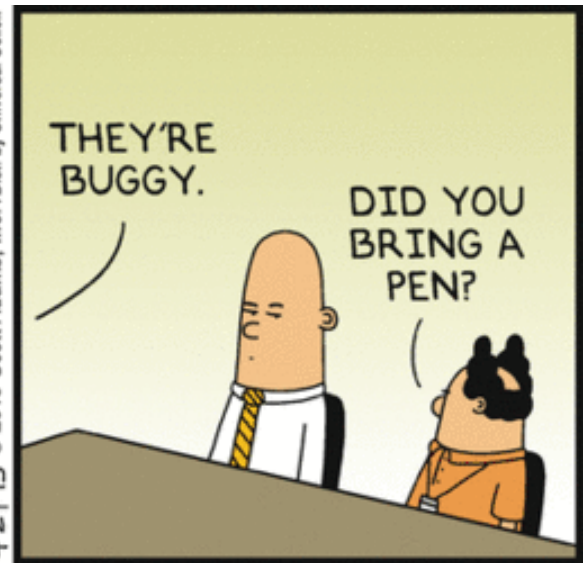
Result: Infections, crypto et. al.



Dilbert.com DilbertCartoonist@gmail.com



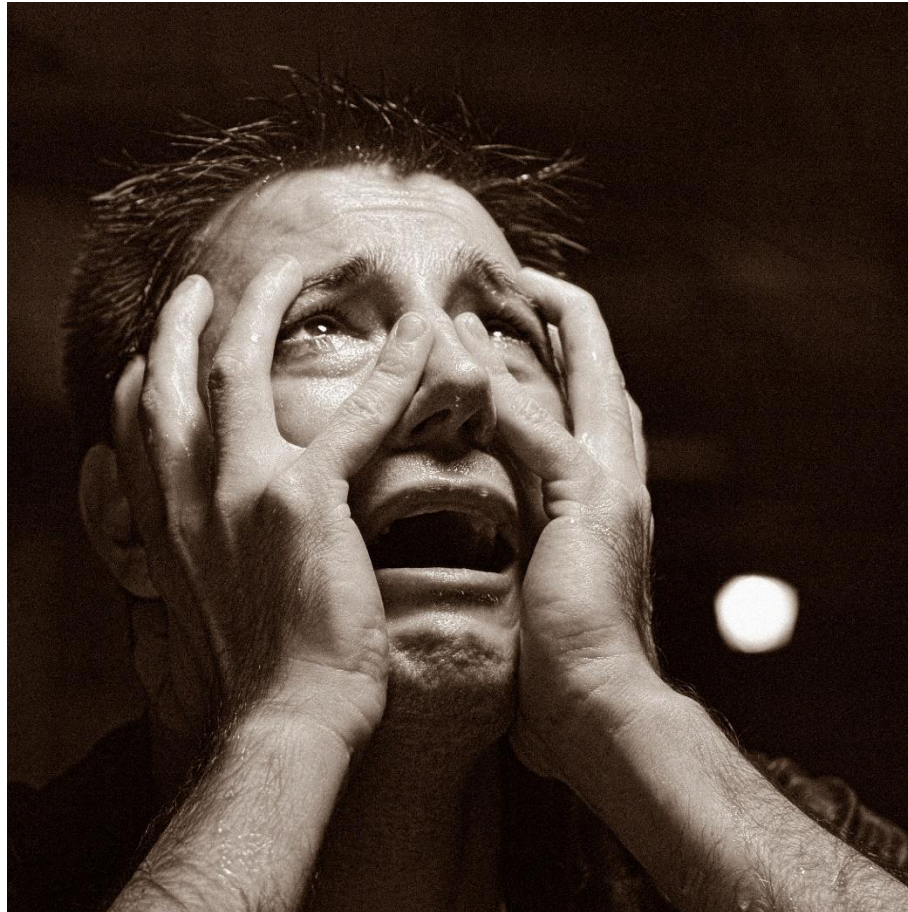
4-24-15 © 2015 Scott Adams, Inc. /Dist. by Universal Uclick



Diversity in the Workplace



REDW_{LLC} We were sitting ducks...



1. Understand our existing culture and capacities
2. Select solution, validate & perform due diligence
3. Establish budget and obtain funds
4. Formulate a plan and schedule
5. Present to ITGC & Board of Directors for approval
6. Begin rollout & solicit feedback
7. Create policy for compliance, enforcement & sanctions
8. Plan for reporting and analysis of results
9. Incorporate new behavior into firm culture

Figure 1. Magic Quadrant Security Awareness Computer-Based Training



Figure 1. Magic Quadrant for Security Awareness Computer-Based Training



Source: Gartner (October 2017)

1. A continuous education and assessment program
2. Immediate assessment and feedback
3. A more robust process for onboarding traditional employees and remote employees
4. A new process for onboarding Independent Contractors and Temporary workers
5. Educational time logged to a new time keeping service code
6. Monthly reporting to Tech Champions and Department Heads on compliance and education
7. Monthly reporting to the ITGC and the Board of Directors

REDW LLC Cybersecurity Education Schedule

| | Quarter 4 | | Quarter 1 | | | Quarter 2 | | | Quarter 3 | | | Quarter 4 |
|------------------------------|--|----------------------------|--|-----------------------------|----------------------------|---|---|--------------------------------|------------------------------|---------------------------|-------------------------------|---|
| Activity | November 2015 | December 2015 | January 2016 | February 2016 | March 2016 | April 2016 | May 2016 | June 2016 | July 2016 | August 2016 | September 2016 | October 2016 |
| Communications | Send Initial Internal Communication to staff | | | | | Send Midcycle Internal Training Program Successes to Date | | | | | | Send End of Cycle Internal Training Program Successes to Date |
| PhishGuru Campaign | Blind Phish for Baseline | | Phish w/AutoEnroll - Email Quota - URL Training AutoEnroll | | Phish - eFaxx | | Phish w/AutoEnroll - Package Delivery - Anti-Phishing Phil AutoEnroll | | Phish - Password | | Phish - Virus Alert | |
| Training Platform Assignment | Train - Email Security (didn't train this month) | Train - Safer Web Browsing | Train Non-Clickers - URL Training | Train - Physical Security | Train - Social Engineering | Train - Security Beyond the Office | Train Non-Clickers - Anti-Phishing Phil | Train - Mobile Device Security | Train - Safe Social Networks | Train - Password Security | Train - Security Essentials | Train - PII |
| Training Reminders | November 15 and November 25 | December 11 and 21 | January 15 and January 25 | February 15 and February 25 | March 16 and March 25 | April 16 and April 25 | May 15 and May 25 | June 15 and June 25 | July 15 and July 25 | August 15 and August 25 | September 16 and September 25 | October 16 and October 25 |
| CyberStrength Assessment | CyberStrength | | | | | Short CyberStrength | | | | | CyberStrength | |



Education & Assessment

"Amateurs hack systems,
professionals hack people"

Bruce Schneier

1. CyberStrength

- Library of 20 Security Awareness Training Modules with in-line assessments (10 - 20 minutes)
- Library of 180+ canned questions to build custom Security Awareness Assessments
- Create custom questions for any type of assessment such as general technology literacy

2. PhishGuru / ThreatSIM

- Library of 100+ phishing emails in 8 categories along with a custom option.
- PhishAlarm / PhishAnalyzer

REDW LLC CyberStrength Training Assignments



Avoiding Dangerous Attachments

Identify and avoid dangerous email attachments



Avoiding Dangerous Links

Recognize common email traps and avoid dangerous links



Data Entry Phishing

Learn to identify and avoid scams that request personal or sensitive data



Data Protection and Destruction

Use portable storage safely and properly discard sensitive data



Email Security

Learn to identify phishing emails, dangerous attachments, and other email scams.



General Data Protection Regulation

Learn how protecting personal data changes under the European General Data Protection Regulation.



Introduction to Phishing

Recognize email traps and avoid phishing scams



Mobile App Security

Learn how to judge the safety of mobile apps.



Mobile Device Security

Use important physical and technical safeguards to protect your devices and your data.



Password Policy

Learn how to create passwords compliant with your company's policy.



PCI-DSS

Recognize warning signs and improve security of credit card data



Physical Security

Learn how to protect people and property.



PII

Protect confidential information about yourself, your employer and your customers



Protected Health Information

Learn why and how you should safeguard Protected Health Information (PHI).



Protecting Against Ransomware

Learn to recognize and prevent ransomware attacks.



Safe Social Networks

Learn how to use social networks safely and responsibly.



Safer Web Browsing

Stay safe on the Internet by avoiding risky behavior and common traps



Security Beyond the Office

Avoid common security mistakes while working at home or on the road.



Security Essentials

Recognize security issues commonly encountered in daily business and personal activities.



Security Essentials: Executive

Recognize and avoid threats encountered by senior managers at work and at home



Social Engineering

Recognize and avoid social engineering scams



Travel Security

Explore how to keep data and devices safe when working in airports, in hotels, at conferences, and in other public spaces



URL Training

Learn how to spot fraudulent URLs



USB Device Safety

Protect yourself, data, and systems when using USB devices



Anti-Phishing Phil

Learn how to spot phishing attacks by identifying fraudulent URLs.



Anti-Phishing Phyllis

Learn how to recognize phishing emails by identifying red flags.

CyberStrength Assessment Library

[+ NEW](#) [ASSIGN](#)

[FILTER](#) [COLUMNS](#)

| | Name | Pr... | Description | Type | Modified | Status |
|--------------------------|---------------------------|-------|--------------------------------------|---------------|------------|----------|
| <input type="checkbox"/> | REDW TechLit - Physical 1 | | REDW Technology Literacy Asses... | Admin Defined | 06/25/2016 | Approved |
| <input type="checkbox"/> | REDW TechLit - Physical 2 | | REDW Technology Literacy Asses... | Admin Defined | 06/25/2016 | Approved |
| <input type="checkbox"/> | REDW TechLit - VDI 2 | | REDW Technology Literacy Asses... | Admin Defined | 06/25/2016 | Approved |
| <input type="checkbox"/> | REDW TechLit - VDI 1 | | REDW Technology Literacy Asses... | Admin Defined | 06/25/2016 | Approved |
| <input type="checkbox"/> | Security on the Go | | Do you know how to protect your d... | Predefined | 06/25/2016 | Draft |
| <input type="checkbox"/> | Protecting Personal Data | | Do you know how to prevent perso... | Predefined | 06/25/2016 | Draft |
| <input type="checkbox"/> | Online Safety | | Do you know how to safely explore... | Predefined | 06/25/2016 | Draft |
| <input type="checkbox"/> | Phishing | | Do you know how to spot and reac... | Predefined | 06/25/2016 | Draft |
| <input type="checkbox"/> | Protected Health Info | | How much do you know about HIP... | Predefined | 06/25/2016 | Draft |
| <input type="checkbox"/> | Payment Card Industry | | How much do you know about PCI... | Predefined | 06/25/2016 | Draft |
| <input type="checkbox"/> | Security Safeguards | | How much do you know about pas... | Predefined | 06/25/2016 | Draft |

0 entries selected

1 of 1

showing 11 of 11

[EDIT](#) [COPY](#) [DELETE](#)



REDW LLC Email Notification of Assignment

From: Tech Education [mail to:TechEducation@REDW.COM]
Sent: January 15, 2018 9:58 AM
To: Jennifer Moreno [mail to:JMoreno@redw.com]
Subject: You have been assigned Cyber Security Training

Hi Jennifer,

The REDW ITGC Technology & Security Awareness Platform (a.k.a. Wombat) provides educational tools to assess and improve your technology and cyber security skills both at work, and at home.

You have an assignment awaiting your completion. Please click on the link below to start your assignment, 2018 January - Dangerous Links, which is due by 02/02/2018.

<https://redw.securityeducation.com/ticketAuth/a56af384983841edb29ed5e425fdd32c>

Once you have finished the cyber security assignment please enter your time to the Administrative client and use the Technology Training service code 90024.

If you have any questions or any feedback, please reach out to us at techeducation@redw.com.

Thank you,
REDW Tech Education Team

Choose one of the following answers:

As you are typing a long email, Outlook freezes and become unresponsive, but your computer otherwise seems seems OK. You don't want to lose your work, so what can you do?

Use the Snipping Tool to make a copy of your work

Use Task Manager to end Outlook and hope that a draft of your work has been saved

Invoke the magical power of digital deities to heal Outlook

All of the above



Use the Snipping Tool to make a copy of your work

Use Task Manager to end Outlook and hope that a draft of your work has been saved

Invoke the magical power of digital deities to heal Outlook

All of the above

Good job!

The best first step is to take a Snip of your work. The other options might work, but often don't

Use Task Manager to end Outlook and hope that a draft of your work has been saved



Invoke the magical power of digital deities to heal Outlook

All of the above

Oops!

The best first step is to take a Snip of your work. The other options might work, but often don't

Next

1. ALL new employees, temporary and independent contractors read & sign a 'Welcome to REDW Technology' document before they can access REDW Protected Data.
2. Enroll all new workers in 4 training modules to be completed the first week
 - URL Training
 - PII
 - Security Essentials
 - Anti-Phishing

Bi-annually Firm-wide CyberStrength Assessments

Twenty (20) Security Awareness Training modules

- Training modules to be assigned bi-monthly
- Allow 3 weeks to complete with a completion reminder after 2 weeks

Annual training and assessment schedule

1. Technology Literacy Assessment (completed)
 - Assigned to new hires after 30 days
2. Future REDW Technology Literacy Assessments
3. Can customize assessment questions



Phishing

"Phishing is a major problem because there really is no patch for human stupidity"

Mike Danseglio Microsoft

1. CyberStrength

- Library of 17 Security Awareness Training Modules with in-line assessments (15 - 20 minutes)
- Library of 156 canned questions to build custom Security Awareness Assessments
- Create custom questions for any type of assessment such as general technology literacy

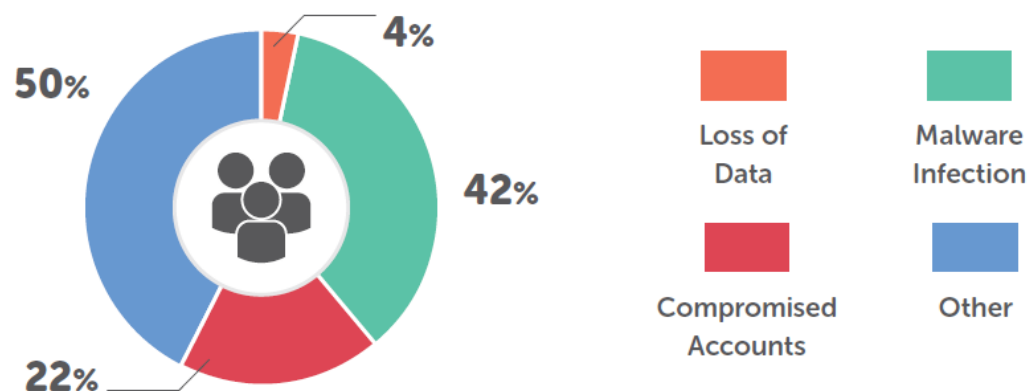
2. PhishGuru / ThreatSIM

- Library of numerous phishing email templates in 10 categories along with a custom option.
- PhishAlarm / PhishAnalyzer

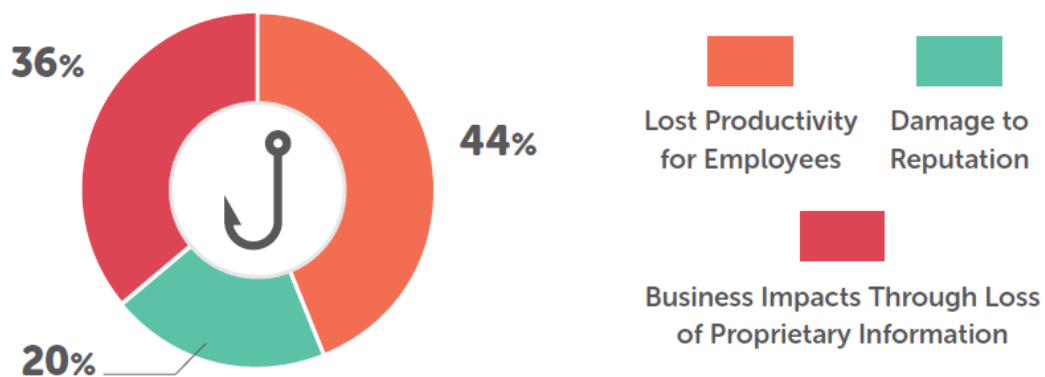
What Is the Impact of Phishing on Your Organization?

The aftermath of phishing attacks can be devastating to an organization, whether through loss of employee productivity, damage to reputation, or money lost. We surveyed security professionals to understand how they viewed the impact of phishing on their organization and how they measured the cost of phishing incidents.

What, if any, of the following impacted your organization?
(choose all that apply)



How do you measure the cost of phishing incidents?



REDW LLC Phishing Schedule

| | Quarter 4 | | Quarter 1 | | | Quarter 2 | | | Quarter 3 | | | Quarter 4 |
|------------------------------|--|----------------------------|--|-----------------------------|----------------------------|---|---|--------------------------------|------------------------------|---------------------------|-------------------------------|---|
| Activity | November 2015 | December 2015 | January 2016 | February 2016 | March 2016 | April 2016 | May 2016 | June 2016 | July 2016 | August 2016 | September 2016 | October 2016 |
| Communications | Send Initial Internal Communication to staff | | | | | Send Midcycle Internal Training Program Successes to Date | | | | | | Send End of Cycle Internal Training Program Successes to Date |
| PhishGuru Campaign | Blind Phish for Baseline | | Phish w/AutoEnroll - Email Quota - URL Training AutoEnroll | | Phish - eFaxx | | Phish w/AutoEnroll - Package Delivery - Anti-Phishing Phil AutoEnroll | | Phish - Password | | Phish - Virus Alert | |
| Training Platform Assignment | Train - Email Security (didn't train this month) | Train - Safer Web Browsing | Train Non-Clickers - URL Training | Train - Physical Security | Train - Social Engineering | Train - Security Beyond the Office | Train Non-Clickers - Anti-Phishing Phil | Train - Mobile Device Security | Train - Safe Social Networks | Train - Password Security | Train - Security Essentials | Train - PII |
| Training Reminders | November 15 and November 25 | December 11 and 21 | January 15 and January 25 | February 15 and February 25 | March 16 and March 25 | April 16 and April 25 | May 15 and May 25 | June 15 and June 25 | July 15 and July 25 | August 15 and August 25 | September 16 and September 25 | October 16 and October 25 |
| CyberStrength Assessment | CyberStrength | | | | | Short CyberStrength | | | | | CyberStrength | |

Pro: obtains the most accurate baseline of behavior

vs.

Con: perceived to be deceptive by actively tricking users

We decided that the seriousness of the threat justified the perceived risk of deceptive practice



emailcenter <emailcenter@maildeliverysystem.net>


 Jennifer Moreno

Thu 3/15

Undelivered eMail

[Retention Policy](#) Email Retention (2 years)

Expires 3/14/2020

 Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.



Our server Detected [19] undelivered mail messages on Thursday, March 15, 2018, awaiting approval to be delivered.

Please note that this may cause mailbox malfunctions. Therefore, follow instruction below:

1. Proceed to [allow messages](#) to Inbox
2. Proceed to [mail cleaning](#) with our admin server.

Note : Messages will be lost if above actions are not taken

Oops! The email you just responded to was a fake phishing email. Don't worry! It was sent to you to help you learn how to avoid real attacks. Please do not share your experience with colleagues, so they can learn too.

John receives an urgent email...

This email looks important. I'd better act quickly.

STOP!

You could have fallen for this email scam. Hackers use emails to steal sensitive information.

This is how scammers try to trick you...

Helpdesk-Mail Alert Confirmation

This E-mail is sent by the HelpDesk Expert for IT Support system for notification and update purposes.
Please click the link below to upgrade your mailbox.

[CLICK HERE](#)

Thank You
HelpDesk Expert

I send you what seems to be an important or interesting message, tempting you to respond right away.

The email will look legitimate, but it's just a disguise. Once you reply with information or click links, I'll have easy access to your data — or your online accounts!

How to protect yourself...

1 Never reveal personal, corporate, or financial data in response to an unsolicited email.

2 Do not click, respond to, or fill in forms in suspicious emails.

Name: SSN:

3 Hover over links to see their true sources.

<http://updates.account-updates.com/t/1412134404>

4 Don't be fooled by logos and familiar brand names. Instead of replying or clicking, type a known address into your browser.

Hmmm...now I'm not sure about this email. I'll check into it before responding.

I could have had access to valuable information! It was only a click away!

To learn more, contact your IT security department.

Oops! The email you just responded to was a fake phishing email. Don't worry! It was sent to you to help you learn how to avoid real attacks. Please do not share your experience with colleagues, so they can learn too.

Stay Alert for Dangerous Attachments

Downloading infected files puts you and your employer at risk



This was a test — a dangerous attachment could have given hackers access to your computer, compromised your company's network, or infected your system with malicious software

Beware of These Warning Signs

- Unsolicited emails that contain attachments
- Random requests to download forms, fill them out, and return them
- Free software or media files that seem too good to be true

Email Safety Tips

- Don't download any attachments in suspicious emails
- Delete suspicious emails with attachments without responding
- Ask your IT department for advice if you're unsure

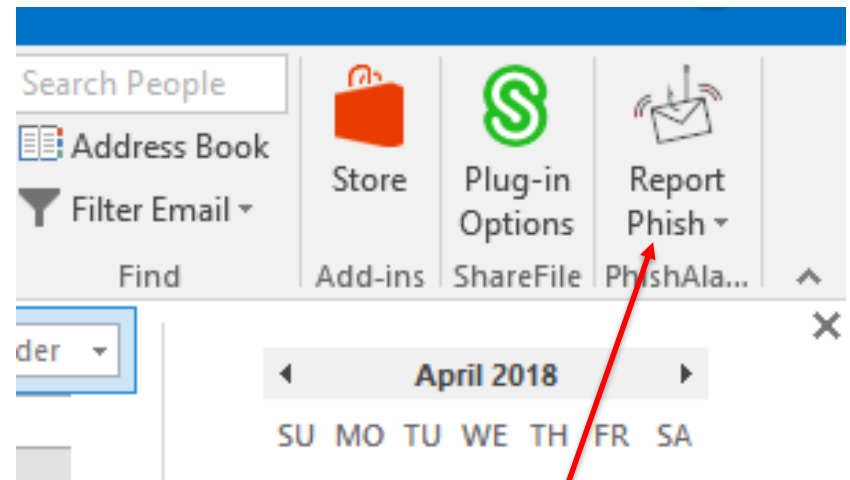
Acknowledge

Auto enrollment for failing a Phish

- Teachable moments provide immediate feedback
- Allow only a few days to complete the auto-enrolled Anti-Phish training module

Auto enrollment for training for underperforming the CyberStrength Assessment

PhishAlarm makes it easy to deal with suspicious emails. Just one-click, and no need to contact tech support..



Outlook Plug-In





analyzer@analyzer.securityeducation.com

Jennifer Moreno

3

9:33 AM

Suspicious: Action needed: Please confirm activity

Retention Policy Email Retention (2 years)

Expires 3/21/2020

i If there are problems with how this message is displayed, click here to view it in a web browser.



ATT00001.txt
284 bytes



headers-03ad51b4-8ddd-4bd2-98ff-1487f21e4a73.txt
3 KB



Action needed: Please confirm activity
Outlook item



2018-03-22

Threat Report Overview

Suspicious:





Reporting

"There is no castle so strong that it cannot be overthrown by money"

Cicero – 63 BC

REDW LLC Individual CyberStrength Assessment Report

Scores By Module

| Module Name | Best Score | Last Score |
|---------------------------------|------------|------------|
| Anti-Phishing Phil | 97% | 97% |
| Anti-Phishing Phyllis | 91% | 91% |
| Email Security | 91% | 91% |
| Passwords | 100% | 100% |
| Safer Web Browsing | 100% | 100% |
| CyberStrength | 100% | 100% |
| PII | 87% | 80% |
| Data Protection and Destruction | 93% | 93% |
| Social Engineering | 100% | 100% |
| URL Training | 91% | 91% |

Page 1 of 2 > >>

User Assignment Status

| Assignment | Status | Modules Remaining |
|------------------------------------|-----------|-------------------|
| Tech Literacy IT | Completed | |
| Dec 2015 - Safer Web Browsing | Completed | |
| Feb 2016 - URL Training | Completed | |
| April 2016 - Email Security | Completed | |
| May 2016 - Anti-Phishing Phil | Completed | |
| June 2016 - Security Essentials | Completed | |
| July 2016 - PII | Completed | |
| August 2016 - Social Engineering | Completed | |
| October 2016 - Physical Security | Completed | |
| REDW 2016 CyberSecurity Assessment | Completed | |

Page 1 of 2 > >>

REDW^{LLC} Module Assignment Completion

REDW

Assignment Details

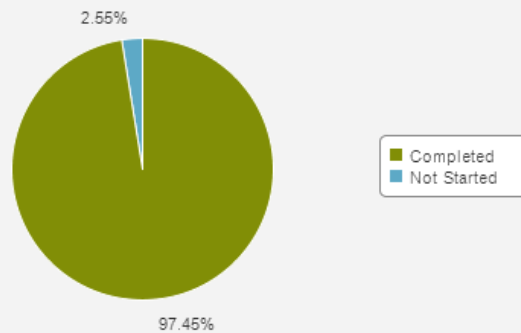
Assignment: 2017 Year End Cyberstrength Assessment

End Date: 01/10/2018

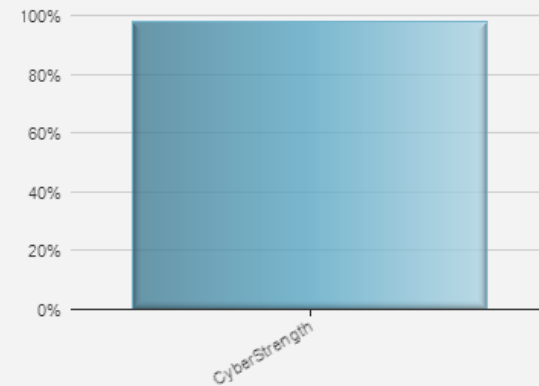
Total Users: 196

[Change Report Criteria](#)

Assignment Status



Completion % By Module



Assignment Completion By User

| First Name | Last Name | Overall | CyberStrength |
|------------|-----------|-----------|---------------|
| Jennifer | Moreno | Completed | Completed |

REDW LLC ThreatSim Aggregate Campaign Report

All Email Campaigns

Recent

Last Week

Last Month

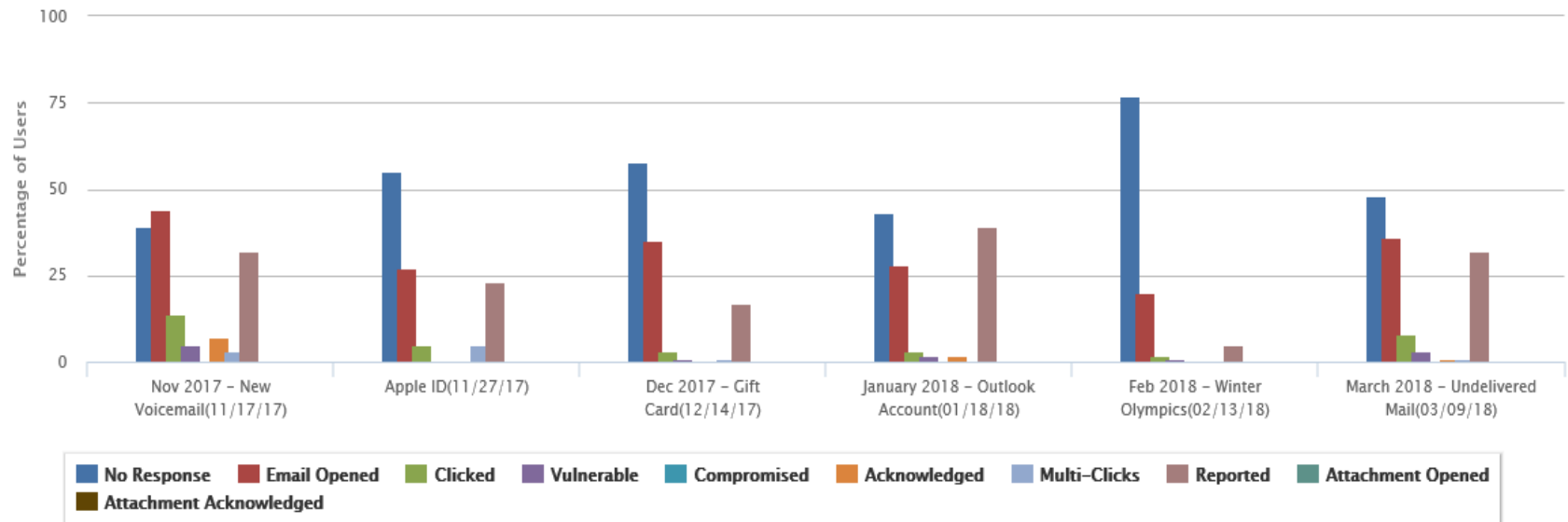
Last Year

Custom Date Range: From

To

Filter

Recent Campaigns



REDW^{LLC} ThreatSim Campaign Details

Campaign Overview

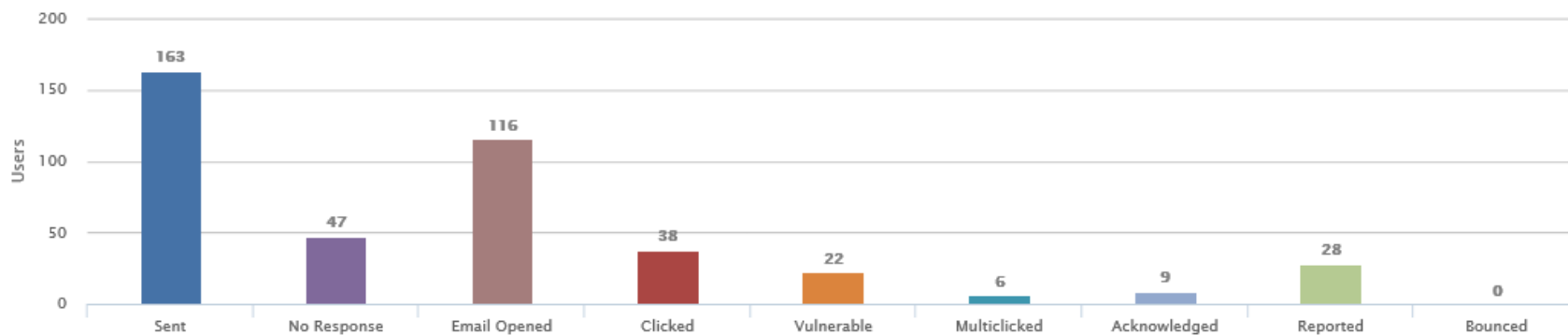
Endpoints

Users

Geographic Distribution

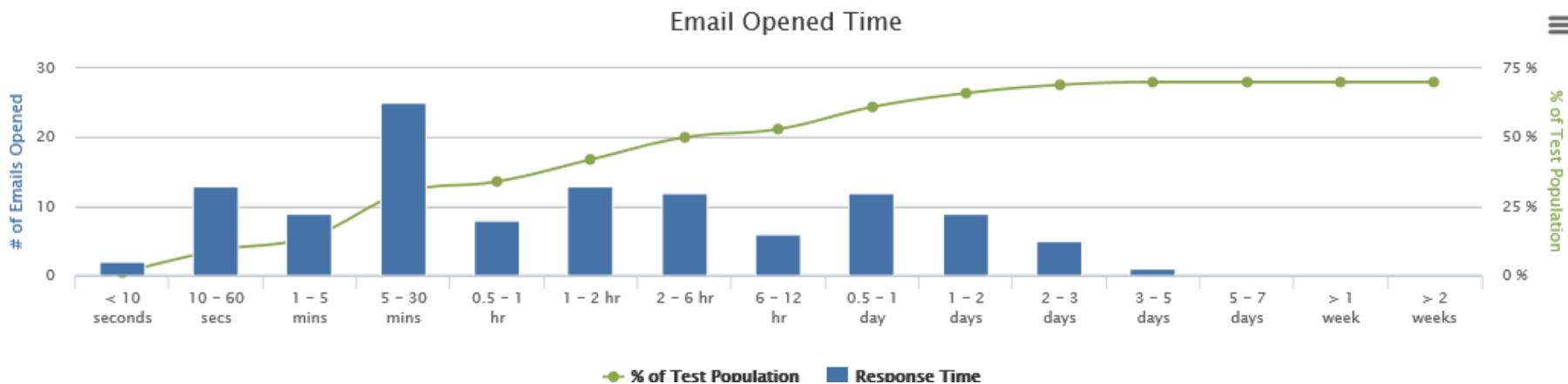
Notes

Campaign Details



Campaign statistics may be delayed up to 5 minutes

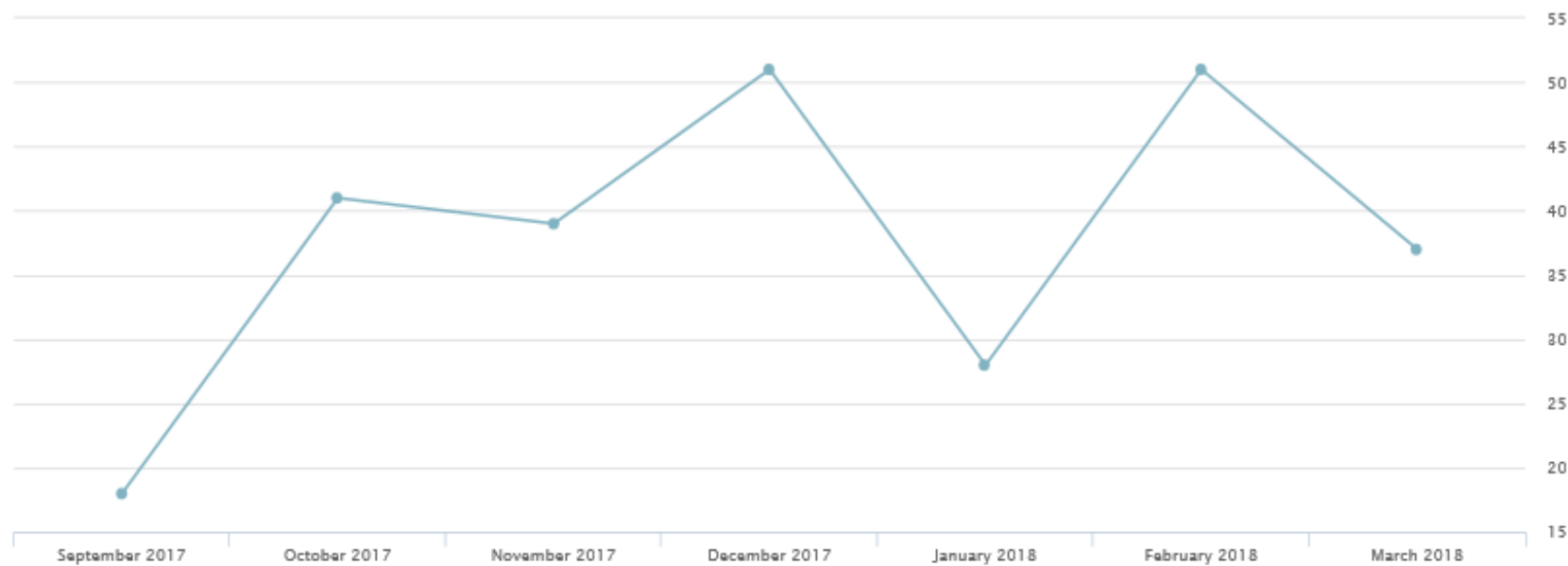
REDW LLC ThreatSim Campaign Detail



Total Potential Phish This Month

37 ↓

down 27% since last month



[Download](#)

REDW LLC PhishAnalyzer Reporting

Likely Phish

16 ↓

down 33% since last month

Suspicious Phish

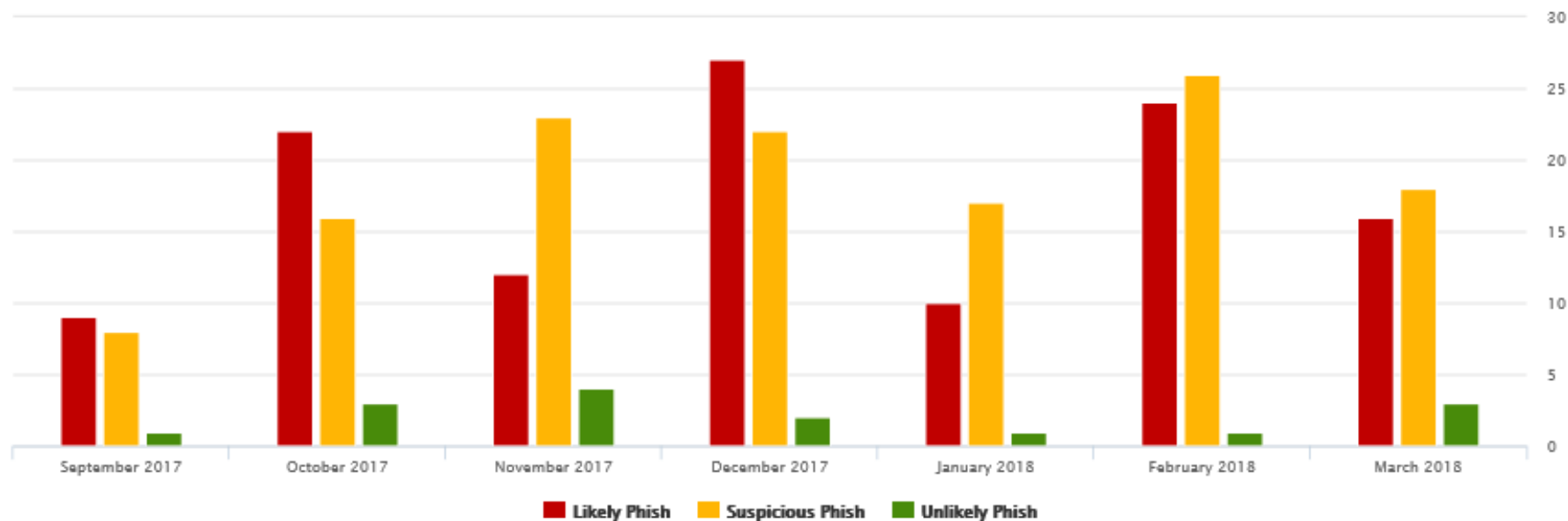
18 ↓

down 31% since last month

Unlikely Phish

3 ↑

up 200% since last month



[Download](#)

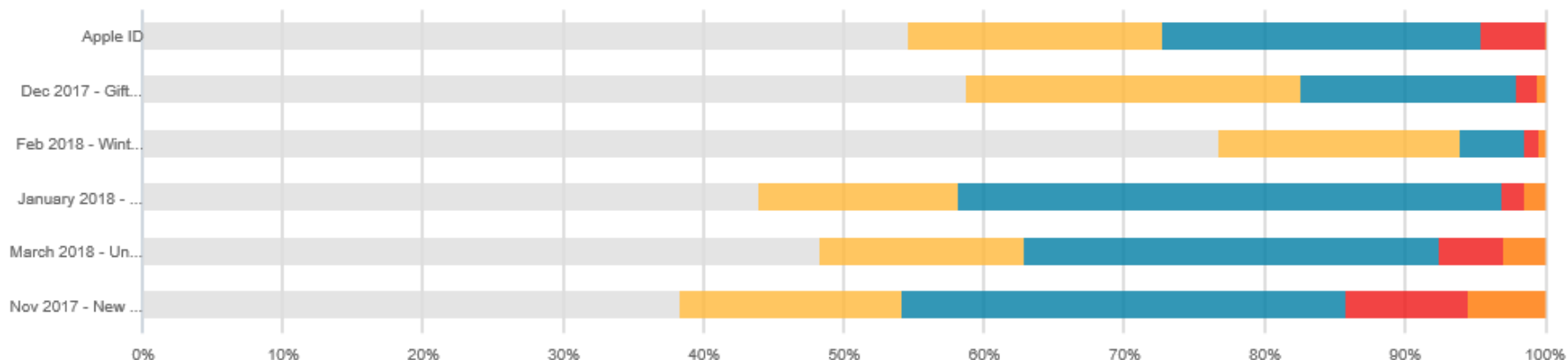
REDW So how's all of this working out?

Campaign Comparison

| Campaign Name | Start Date | End Date | Status | Sent | % Sent | Failure % |
|------------------------------|------------|------------|-----------|------|--------|-----------|
| Nov 2017 - New Voicemail | 2017-11-17 | 2017-12-01 | Completed | 183 | 100% | 14% |
| Apple ID | 2017-11-27 | 2017-12-01 | Completed | 22 | 100% | 5% |
| Dec 2017 - Gift Card | 2017-12-15 | 2017-12-27 | Completed | 189 | 100% | 2% |
| January 2018 - Outlook Ac... | 2018-01-19 | 2018-01-29 | Completed | 198 | 100% | 3% |
| Feb 2018 - Winter Olympic... | 2018-02-14 | 2018-02-24 | Completed | 198 | 100% | 2% |
| March 2018 - Undelivered ... | 2018-03-09 | 2018-03-24 | Sent | 199 | 100% | 8% |

Campaign Performance

■ No Action
 ■ Email Viewed
 ■ Email Reported
 ■ Link Clicked
 ■ Vulnerable

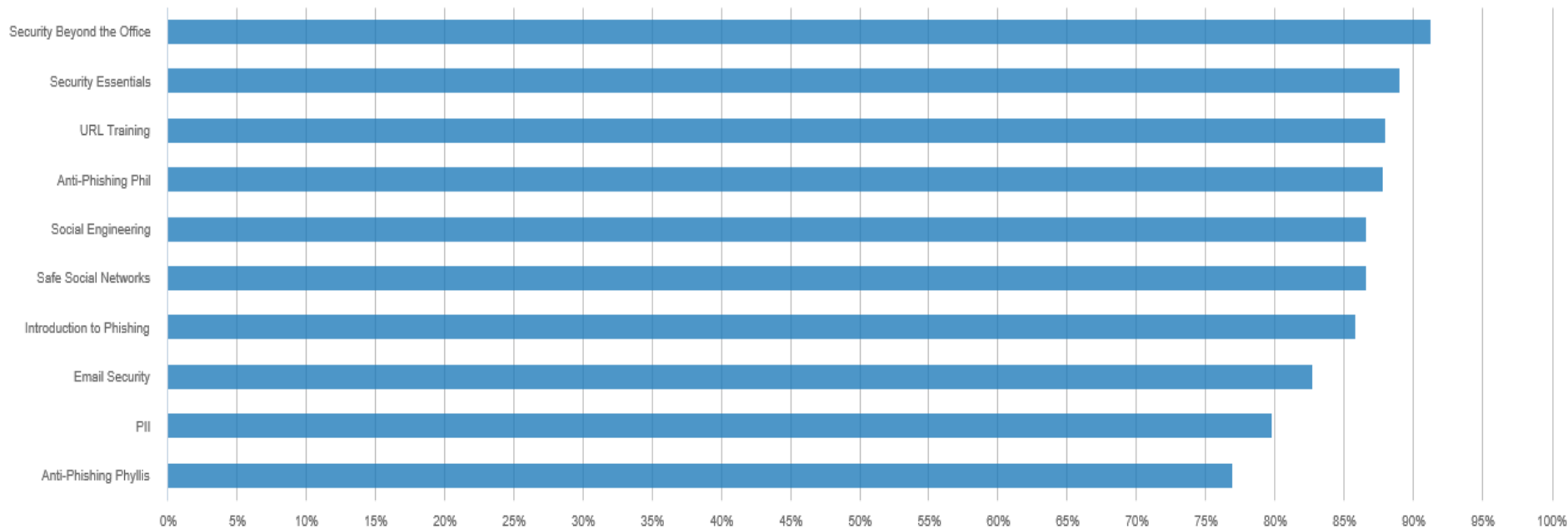


REDW LLC Making the grade in 2017: A- 91%

| Summary | | | | | | |
|---------|--------------|-----------------|-----------------------------|-------------------|------------------------|-----------------------|
| Modules | Unique Users | Module Attempts | Average Attempts per Module | Modules Completed | % of Modules Completed | Overall Average Score |
| 19 | 189 | 1,099 | 58 | 1,053 | 96 | 91 |

Visualization

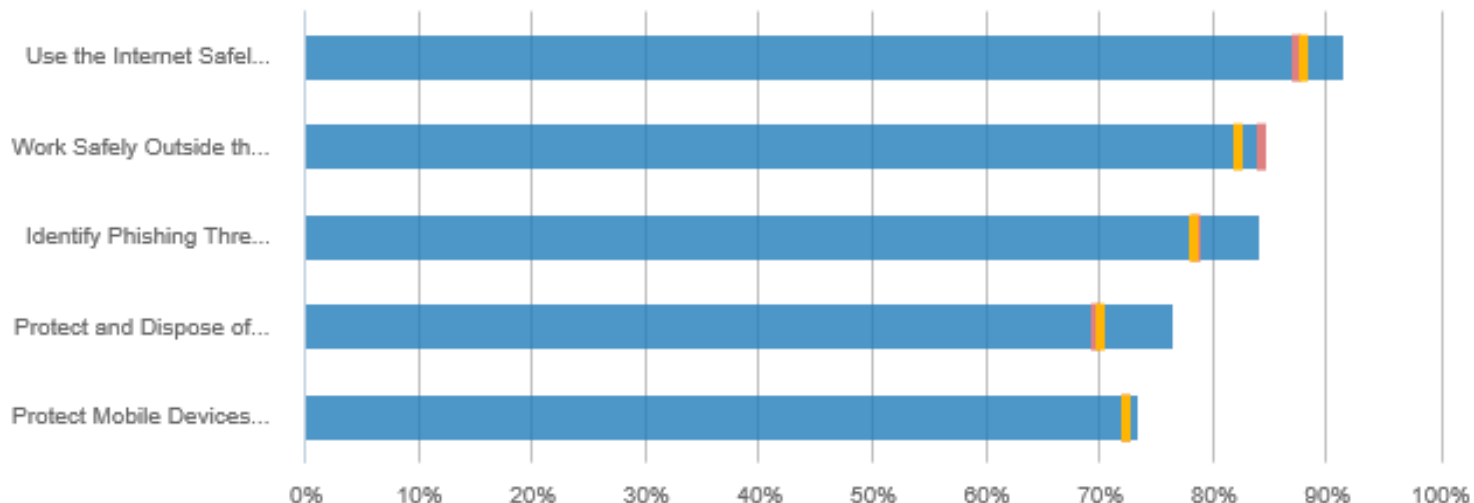
Average Score By Module



REDW LLC Assessing our Risk – Where do we need improvement?

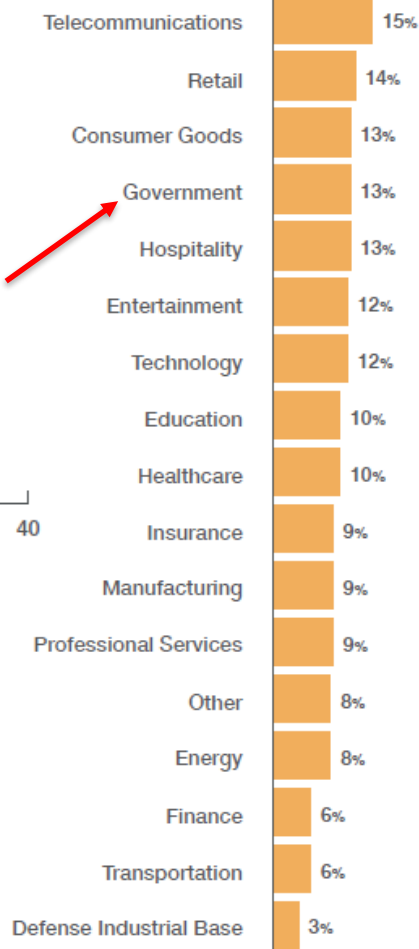
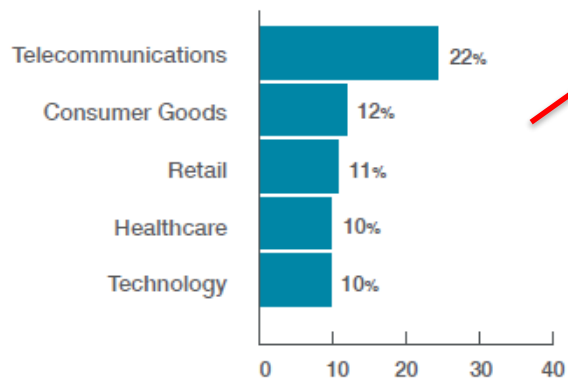
| Category Information | | | |
|--|-------------|-------------|---------------|
| Category | % Correct ▲ | % Incorrect | Average Score |
| Protect Mobile Devices and Information | 74% | 26% | 73% |
| Protect and Dispose of Data Securely | 77% | 23% | 71% |
| Identify Phishing Threats | 84% | 16% | 85% |
| Work Safely Outside the Office | 84% | 16% | 91% |
| Use the Internet Safely | 92% | 8% | 93% |
| Protect Against Physical Risks | 93% | 7% | 96% |

Lowest Scores (By Category)



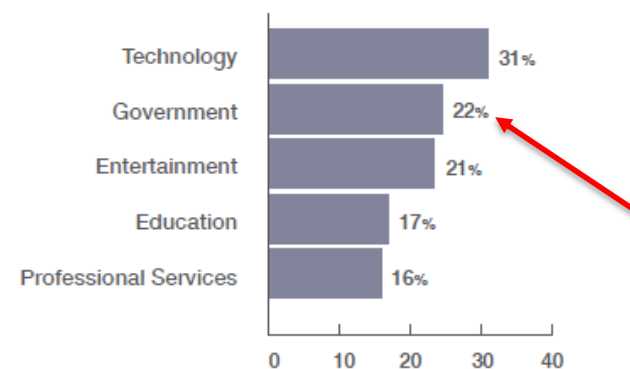
Average Click Rates by Industry

Consumer Click Rates (9% average)

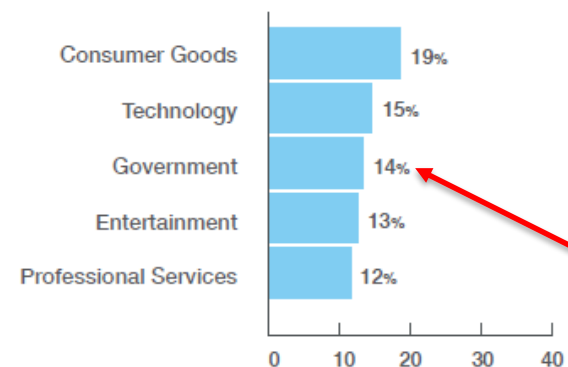


Worst Performing Industries by Template Type

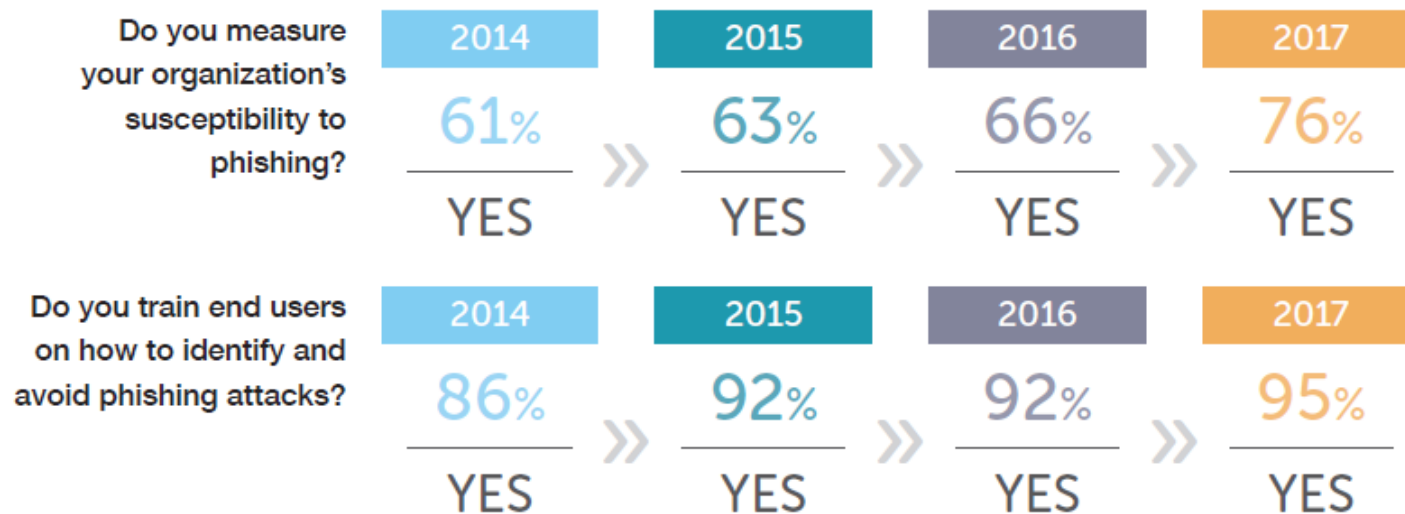
Commercial Click Rates (12% average)



Corporate Click Rates (10% average)



REDW Wombat State of the Phish 2018



54%

of infosec professionals surveyed said they have been able to quantify a reduction in phishing susceptibility based on their training activities.

A 4% increase from 2016

Consequence Models

45%

of organizations said there are ramifications if their users continue to click on simulated phishing attacks.



What types of consequences are enforced in your organization?

We asked infosec professionals about the types of consequences (if any) they have in place to incentivize employees to avoid becoming 'repeat offenders.' *(Note: Multiple answers were permitted.)*

74%

Counseling
from Manager

25%

Removal of
Access to Systems

11%

Termination

5%

Monetary Penalty

1. Understand the prevailing culture
2. Educate leadership on the risk of uneducated workers
3. Reach out and discuss ideas with every department, every constituency
4. Sell the program by reminding workers that this will help them personally
5. Understand and plan for generational differences about personal privacy
6. Stand firm on what you believe your firm minimally needs
7. Plan early to deal with non-compliance with meaningful sanctions
8. Zero tolerance for those who fail to complete remedial programs
9. Accept that no software is perfect, and clearly understand limitations
10. Measure and report success as well as failure



2008 – We hoped for the best...



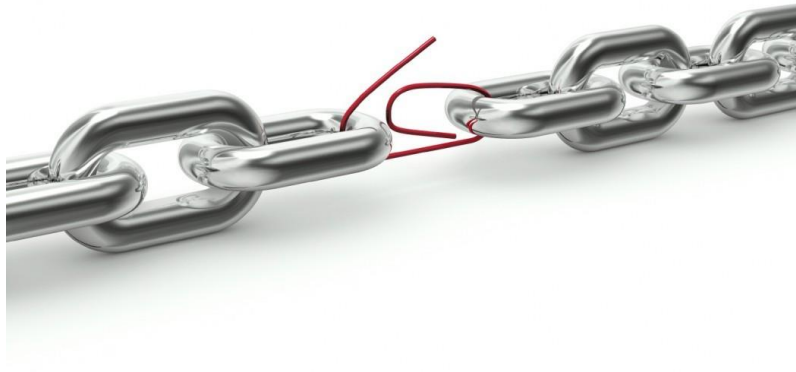
"On the Internet, nobody knows you're a dog."



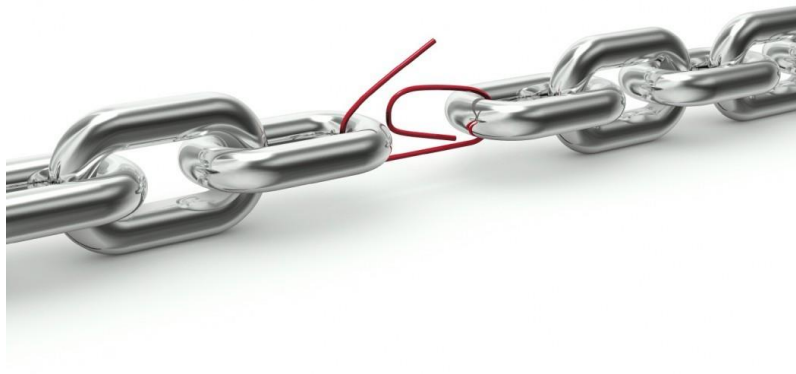
2018 – We prepare for the worst...

"We only need to be lucky once.
You need to be lucky every time"

*The IRA to Margaret Thatcher,
after a failed assassination attempt.*

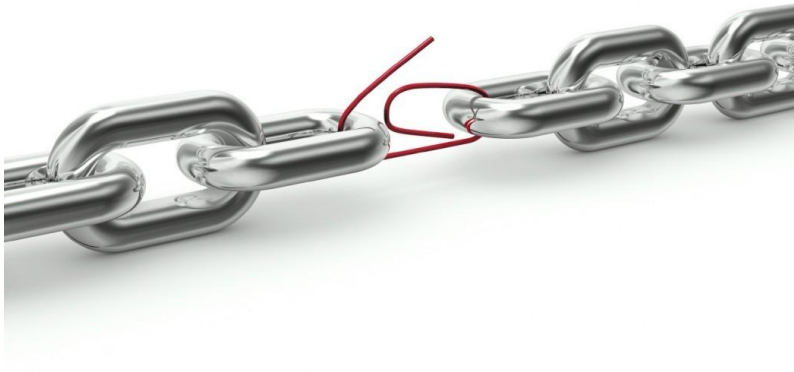


The 5 facts every
Government
Administrator
should know

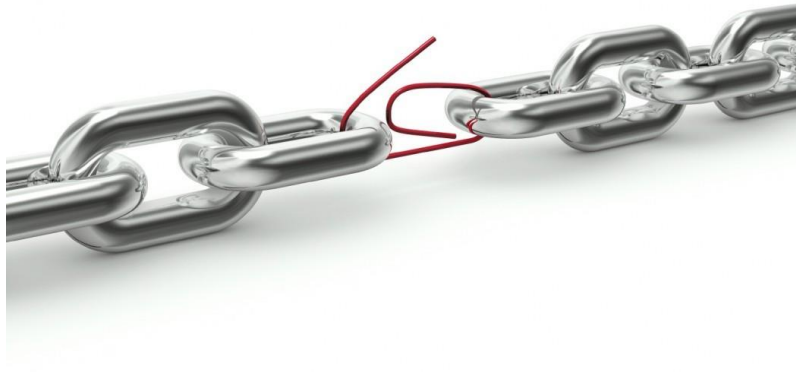


1. Cyber-attacks and security breaches *will* happen, and *will* adversely impact your organization.

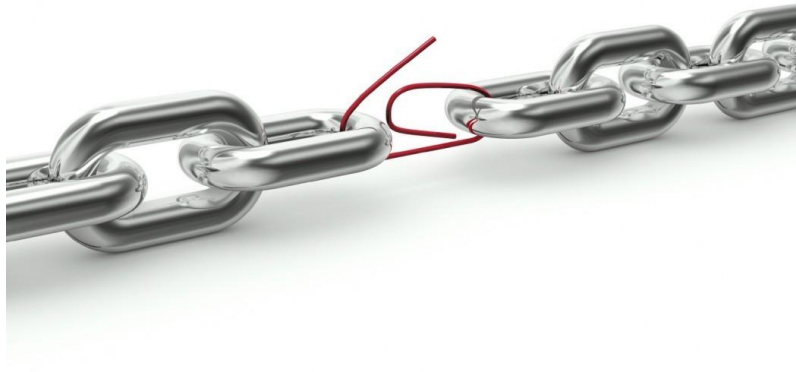
The average cost of a breach is *\$4.9 million*



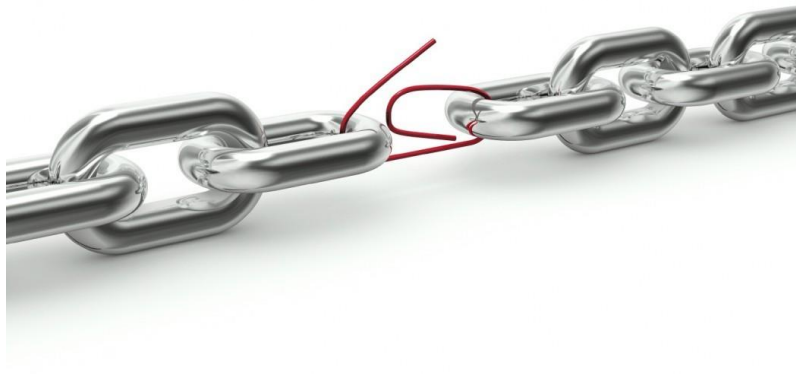
2. Over 60% of all data breaches originate from unauthorized access by a current or former employee, or third-party suppliers



3. Compliance with one or more government regulatory standards (e.g. ISO 27001, NIST 800-171) is good, *but not sufficient to ensure real cybersecurity*



4. Cyber liability insurance premiums are *significantly increasing in cost* and often *do not cover all damages* caused by a cyber breach.



5. To achieve *real information security and data resilience*, it is vital to combine Managed Monitoring, Detection, and Response services with *comprehensive disaster recovery and business continuity plans*.

1. Find out where you really stand. Perform or contract an assessment of your cyber-resilience.
2. Inventory all data, especially regulated (PII or PHI) personal data. Expire, or prune all unneeded data per retention policy
3. Regularly practice and update your Security Incident Response Plan
4. The most valuable investment is the security awareness and education of employees, contractors & partners
5. Set the right tone at the top. Leadership matters.
6. Secure sufficient Cyber-Liability insurance coverage
7. Continuous monitoring & assessment is vital

REDW^{LLC} thank you!



Jennifer Moreno CISA

Senior Manager of GRC CyberHealth

505.998.3239

jmoreno@redw.com



Marcus Clarke

Principal – Technology & CyberHealth

505.998.3224

mclarke@redw.com