vertical®
COMMUNICATIONS

Security As A Service

The Crucial Hidden Factor in Selecting Cloud Vendors

Agenda

01 Cost of Failed Security

02 Security Is Not a Wall

03 Security As A Service

04 What Makes Up SaaS?

05 Certifications As A Service

06 Getting Good SaaS

07 Questions?

vertical®
COMMUNICATIONS

Cost of Failed Security

The Cost of Failed Security

IBM Security

The Cost of Failed Security

IBM Security

$3,920,000

Average total data breach cost

The Cost of Failed Security

IBM Security

$3,920,000

Average total data breach cost

$8,190,000

US Average Cost

vertical
COMMUNICATIONS

The Cost of Failed Security

IBM Security

$3,920,000

Average total data breach cost

$8,190,000

US Average Cost

vertical
COMMUNICATIONS

Security Breach Example

This is Mike.

Mike Runs an international shipping business.

Mike has 200 employees.

Mike’s recording archive just got hacked.

Security Breach Example

This is Mike.

Mike Runs an international shipping business.

Mike has 200 employees.

Mike's recording archive just got hacked.

Mike's CIO:
"Over 25,000 records were compromised on a system we were told was secure."

Source: Ponemon Institute Study, 2018

Security Breach Example

This is Mike.

Mike Runs an international shipping business.

Mike has 200 employees.

Mike's recording archive just got hacked.

Mike's CIO:
"Over 25,000 records were compromised on a system we were told was secure."

Mike's Lawyer:
"We will likely get sued by all of our customers. This could cost us $4 million. "

Source: Ponemon Institute Study, 2018

Security Breach Example

This is Mike.

Mike Runs an international shipping business.

Mike has 200 employees.

Mike's recording archive just got hacked.

Mike's CIO:
"Over 25,000 records were compromised on a system we were told was secure."

Mike's Lawyer:
"We will likely get sued by all of our customers. This could cost us $4 million. "

Mike's CFO:
"Don't forget potential fines from the EU. They could charge up to 4% of our top-line revenue."

Source: Ponemon Institute Study, 2018

Security Breach Example

This is Mike.

Mike Runs an international shipping business.

Mike has 200 employees.

Mike's recording archive just got hacked.

Mike's CIO:
"Over 25,000 records were compromised on a system we were told was secure."

Mike's Lawyer:
"We will likely get sued by all of our customers. This could cost us $4 million. "

Mike's CFO:
"Don't forget potential fines from the EU. They could charge up to 4% of our top-line revenue."

Mike's Sales Director:
"I'm worried about our customers. We may lose 2% of our recurring sales from this.

Source: Ponemon Institute Study, 2018

vertical COMMUNICATIONS

Cyber Insurance

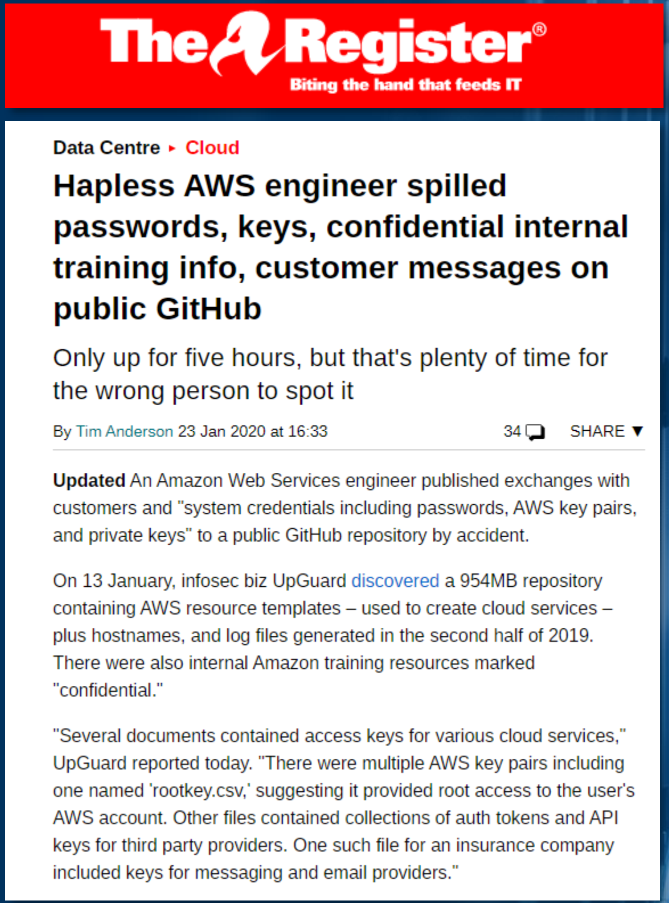
Cyber Insurance Is Not Covering The Cost

Cyber Insurance Is Not Covering The Cost

1

Only covers attacks and intrusions, not human error

Cyber Insurance Is Not Covering The Cost



The Register®
Biting the hand that feeds IT

Data Centre ▸ Cloud

Hapless AWS engineer spilled passwords, keys, confidential internal training info, customer messages on public GitHub

Only up for five hours, but that's plenty of time for the wrong person to spot it

By Tim Anderson 23 Jan 2020 at 16:33 34 SHARE ▼

Updated An Amazon Web Services engineer published exchanges with customers and "system credentials including passwords, AWS key pairs, and private keys" to a public GitHub repository by accident.

On 13 January, infosec biz UpGuard discovered a 954MB repository containing AWS resource templates – used to create cloud services – plus hostnames, and log files generated in the second half of 2019. There were also internal Amazon training resources marked "confidential."

"Several documents contained access keys for various cloud services," UpGuard reported today. "There were multiple AWS key pairs including one named 'rootkey.csv,' suggesting it provided root access to the user's AWS account. Other files contained collections of auth tokens and API keys for third party providers. One such file for an insurance company included keys for messaging and email providers."

1 Only covers attacks and intrusions, not human error

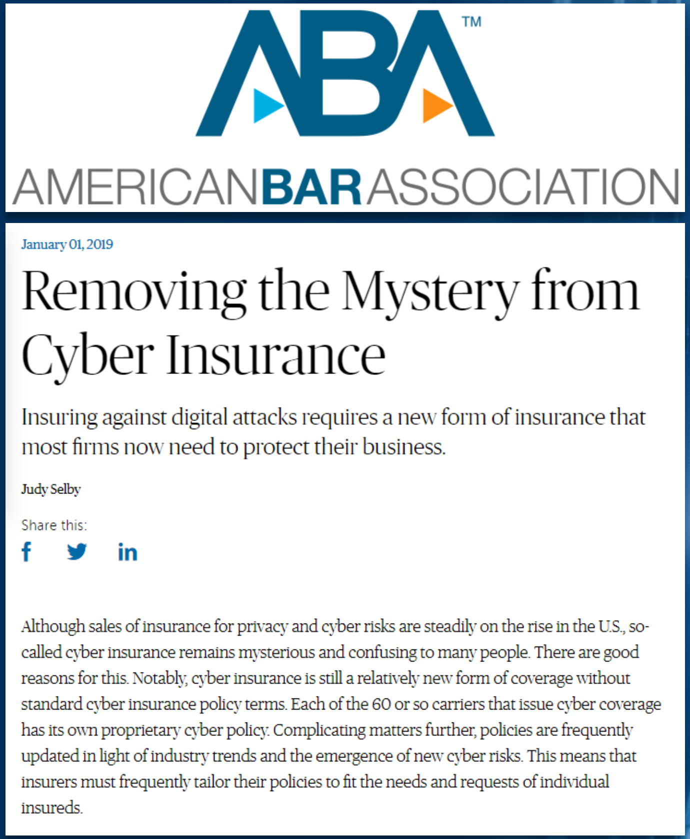
vertical
COMMUNICATIONS

Cyber Insurance Is Not Covering The Cost

1 Only covers attacks and intrusions, not human error

2 Limited time period coverage

Cyber Insurance Is Not Covering The Cost



AMERICAN BAR ASSOCIATION

January 01, 2019

Removing the Mystery from Cyber Insurance

Insuring against digital attacks requires a new form of insurance that most firms now need to protect their business.

Judy Selby

Share this:

Although sales of insurance for privacy and cyber risks are steadily on the rise in the U.S., so-called cyber insurance remains mysterious and confusing to many people. There are good reasons for this. Notably, cyber insurance is still a relatively new form of coverage without standard cyber insurance policy terms. Each of the 60 or so carriers that issue cyber coverage has its own proprietary cyber policy. Complicating matters further, policies are frequently updated in light of industry trends and the emergence of new cyber risks. This means that insurers must frequently tailor their policies to fit the needs and requests of individual insureds.

1. Only covers attacks and intrusions, not human error

2. Limited time period coverage

Cyber Insurance Is Not Covering The Cost

1 Only covers attacks and intrusions, not human error

2 Limited time period coverage

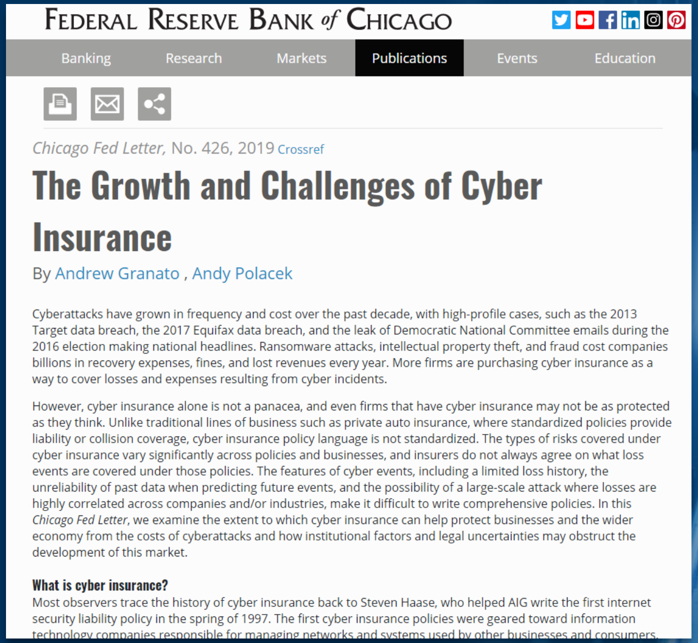
3 Limiting type of damages covered

Cyber Insurance Is Not Covering The Cost

1 Only covers attacks and intrusions, not human error

2 Limited time period coverage

3 Limiting type of damages covered



Chicago Fed Letter, No. 426, 2019 Crossref

The Growth and Challenges of Cyber Insurance

By Andrew Granato , Andy Polacek

Cyberattacks have grown in frequency and cost over the past decade, with high-profile cases, such as the 2013 Target data breach, the 2017 Equifax data breach, and the leak of Democratic National Committee emails during the 2016 election making national headlines. Ransomware attacks, intellectual property theft, and fraud cost companies billions in recovery expenses, fines, and lost revenues every year. More firms are purchasing cyber insurance as a way to cover losses and expenses resulting from cyber incidents.

However, cyber insurance alone is not a panacea, and even firms that have cyber insurance may not be as protected as they think. Unlike traditional lines of business such as private auto insurance, where standardized policies provide liability or collision coverage, cyber insurance policy language is not standardized. The types of risks covered under cyber insurance vary significantly across policies and businesses, and insurers do not always agree on what loss events are covered under those policies. The features of cyber events, including a limited loss history, the unreliability of past data when predicting future events, and the possibility of a large-scale attack where losses are highly correlated across companies and/or industries, make it difficult to write comprehensive policies. In this *Chicago Fed Letter*, we examine the extent to which cyber insurance can help protect businesses and the wider economy from the costs of cyberattacks and how institutional factors and legal uncertainties may obstruct the development of this market.

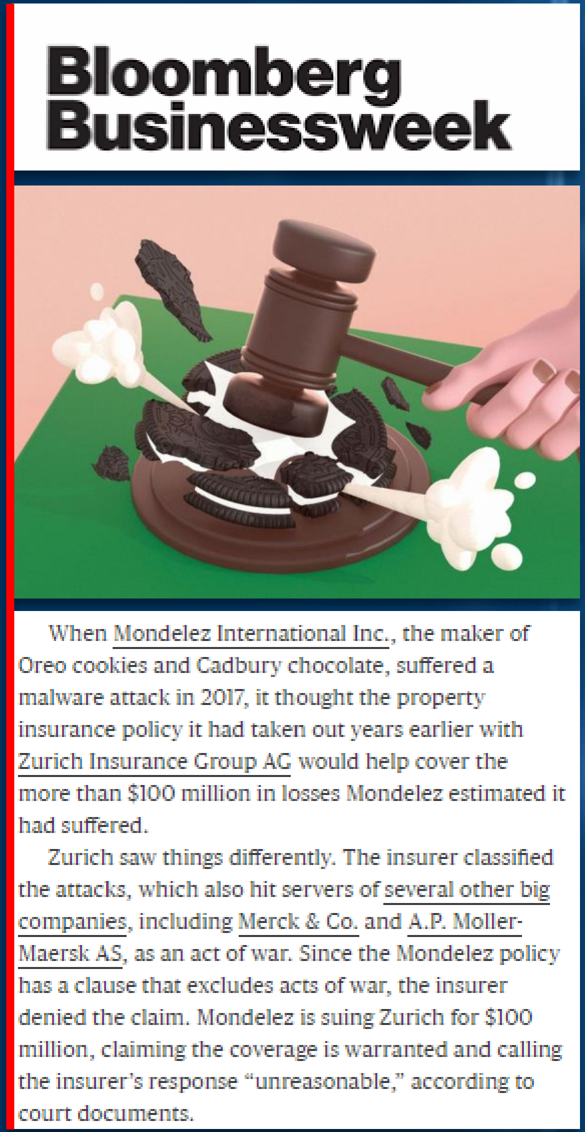
What is cyber insurance?

Most observers trace the history of cyber insurance back to Steven Haase, who helped AIG write the first internet security liability policy in the spring of 1997. The first cyber insurance policies were geared toward information technology companies responsible for managing networks and systems used by other businesses and consumers.

Cyber Insurance Is Not Covering The Cost

1. Only covers attacks and intrusions, not human error
2. Limited time period coverage
3. Limiting type of damages covered
4. Claiming cyber attacks are “act of war”

Cyber Insurance Is Not Covering The Cost



Bloomberg Businessweek

When Mondelez International Inc., the maker of Oreo cookies and Cadbury chocolate, suffered a malware attack in 2017, it thought the property insurance policy it had taken out years earlier with Zurich Insurance Group AG would help cover the more than $100 million in losses Mondelez estimated it had suffered.

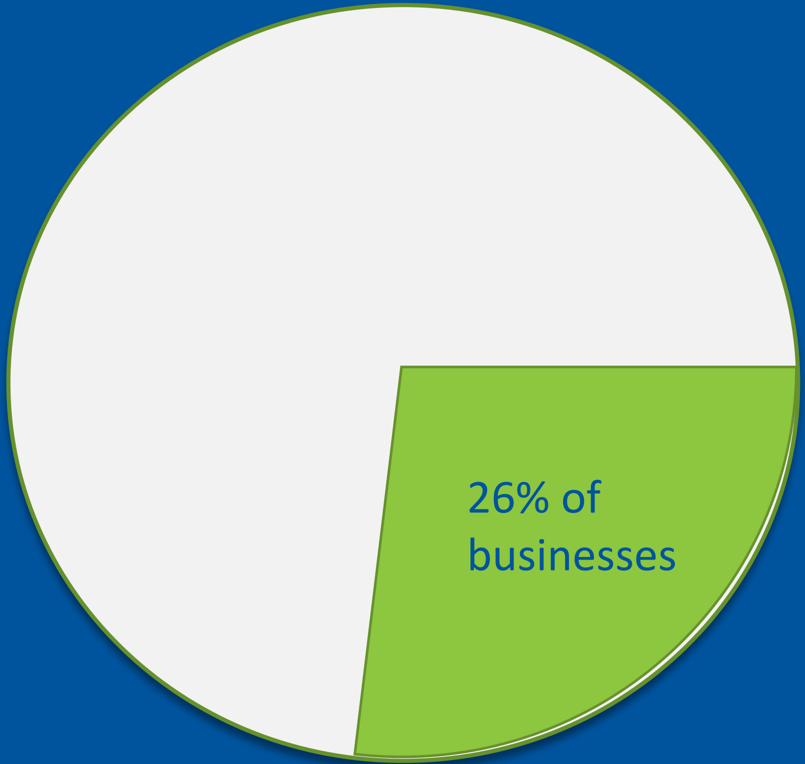
Zurich saw things differently. The insurer classified the attacks, which also hit servers of several other big companies, including Merck & Co. and A.P. Moller-Maersk AS, as an act of war. Since the Mondelez policy has a clause that excludes acts of war, the insurer denied the claim. Mondelez is suing Zurich for $100 million, claiming the coverage is warranted and calling the insurer's response "unreasonable," according to court documents.

1. Only covers attacks and intrusions, not human error
2. Limited time period coverage
3. Limiting type of damages covered
4. Claiming cyber attacks are "act of war"

vertical
COMMUNICATIONS

Likelihood of the Threat?

Businesses that will experience a major security threat[1] in the next 24 months



[1] *Major threat is $1.5 million loss or more.*

62%

% of SMBS who don't have an up to date security strategy

Inc. Magazine and Cisco Survey of 1,377 CEOS, 2018

60%

% of SMBs who will go out of business after a security breach

National Cyber Security Alliance, 2018

What Do We Do About It?

Ensure Your Cloud Provider Includes Adequate Security Measures

What Is Adequate Security?

Security Is Not a Wall

vertical
COMMUNICATIONS

You Can Build The Best Defense Possible

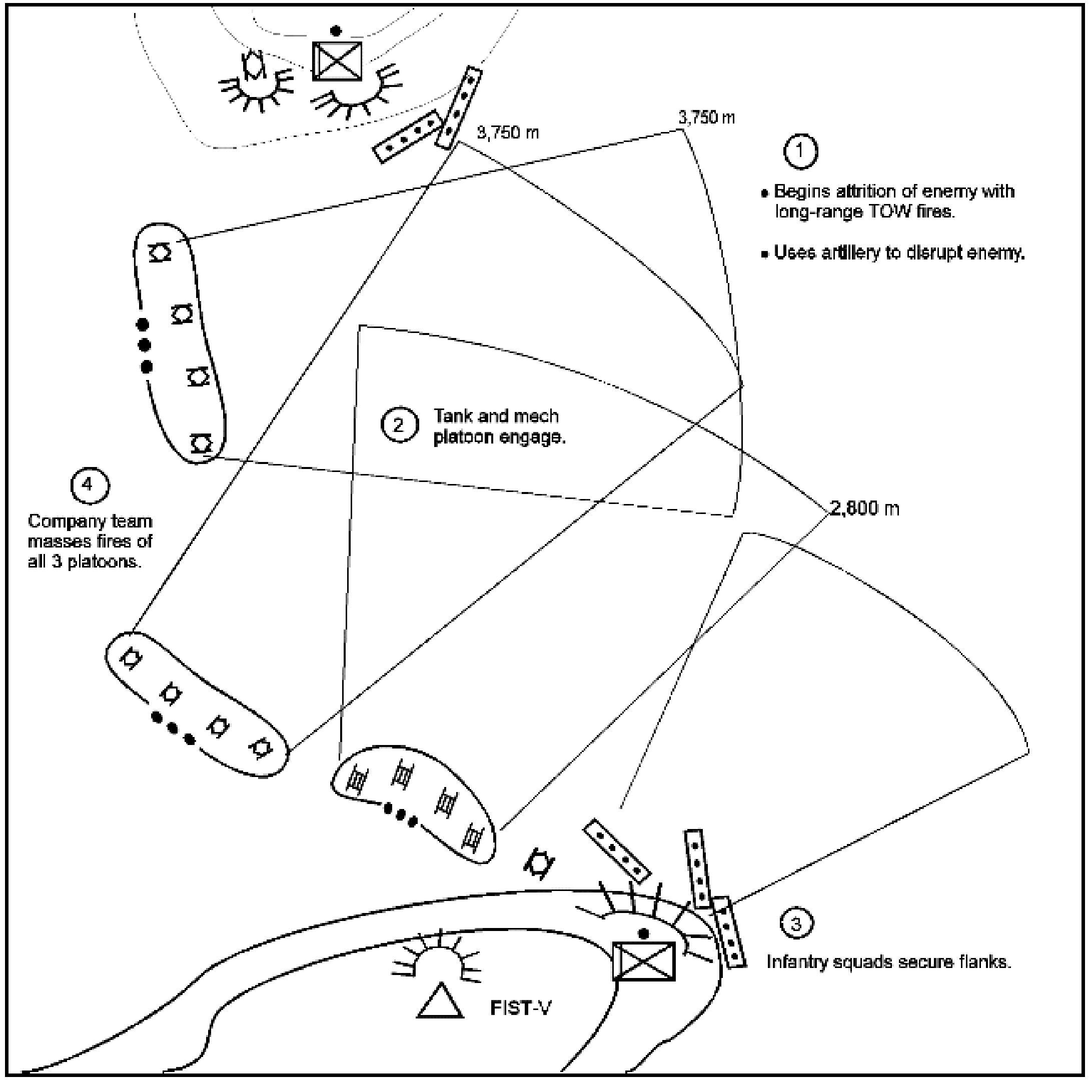
You Can Build The Best Defense Possible

Triple Strand Concertina Wire

- 3 meters high
- 4 meters deep
- Razor wire

Someone Will Find A Simple Way To Defeat It

Security Requires Active Effort


3,750 m
3,750 m
1
Begins attrition of enemy with long-range TOW fires.
Uses artillery to disrupt enemy.
2
Tank and mech platoon engage.
2,800 m
4
Company team masses fires of all 3 platoons.
3
Infantry squads secure flanks.
FIST-V

“Defenses must be **maintained and observed** or else they are not defenses. They are a waste of time.”

Security Isn’t A Feature…

Features

- Encryption
- SRTP
- Password management
- Data center access restriction
- Security standards

Security Isn’t A Feature…It’s A Process

Features

- Encryption
- SRTP
- Password management
- Data center access restriction
- Security standards

Processes

- Software updates
- Real-time monitoring
- Penetration testing
- Access reviews
- Policy updates

Being in the Cloud Can Help Security

“as a Service”
means you can get
ongoing security service

The Value of Security as a Service

vertical
COMMUNICATIONS

Premise Solutions Have A Flaw

Features

- Encryption
- SRTP
- Password management
- Data center access restriction
- Security standards

Premise Solutions Have A Flaw

Features

- Encryption
- SRTP
- Password management
- ~~Data center access restriction~~
- Security standards

Premise Solutions Have A Flaw

Features

- Encryption
- SRTP
- Password management
- ~~Data center access restriction~~
- Security standards

Processes

- Software updates
- Real-time monitoring
- Penetration testing
- Access reviews
- Policy updates

Premise Solutions Have A Flaw

Features

- Encryption
- SRTP
- Password management
- ~~Data center access restriction~~
- Security standards

Processes

- Software updates
- ~~Real-time monitoring~~
- ~~Penetration testing~~
- ~~Access reviews~~
- ~~Policy updates~~

Cloud SaaS Is An Ongoing Relationship

Customer Pays Monthly

Should Get Recurring Value

Look for Proactive Security from Your Cloud Vendor

Expect Active Security Teams Working For Your Client

Look for Proactive Security from Your Cloud Vendor

Expect Active Security Teams Working For Your Client

- Software updates
- Real-time monitoring
- Penetration testing
- Access reviews
- Policy updates

vertical
COMMUNICATIONS

Table Stakes
Just To Play

What Should Be Included?

What Should Be Included?

Dedicated Security Team

- Only job is security
- Real-time monitoring
  - Threats
  - Systems
- Proactive response
- Continuous Planning

What Should Be Included?

Dedicated Security Team

Quick Turnaround Response

- Identify new threats
- Updates released in days
- Customers notified

What Should Be Included?

Dedicated Security Team

Quick Turnaround Response

Continuous Penetration Testing

- Formal red team
- Identifying vulnerabilities
- Testing new software
- Feedback results to security

What Should Be Included?

Dedicated Security Team

Quick Turnaround Response

Continuous Penetration Testing

Published Security Docs

What Should Be Included?

Dedicated Security Team

Quick Turnaround Response

Continuous Penetration Testing

Published Security Docs

Certification Reviews

Certifications

You May Need Certain Certifications

HIPAA

FISMA

PCI-DSS

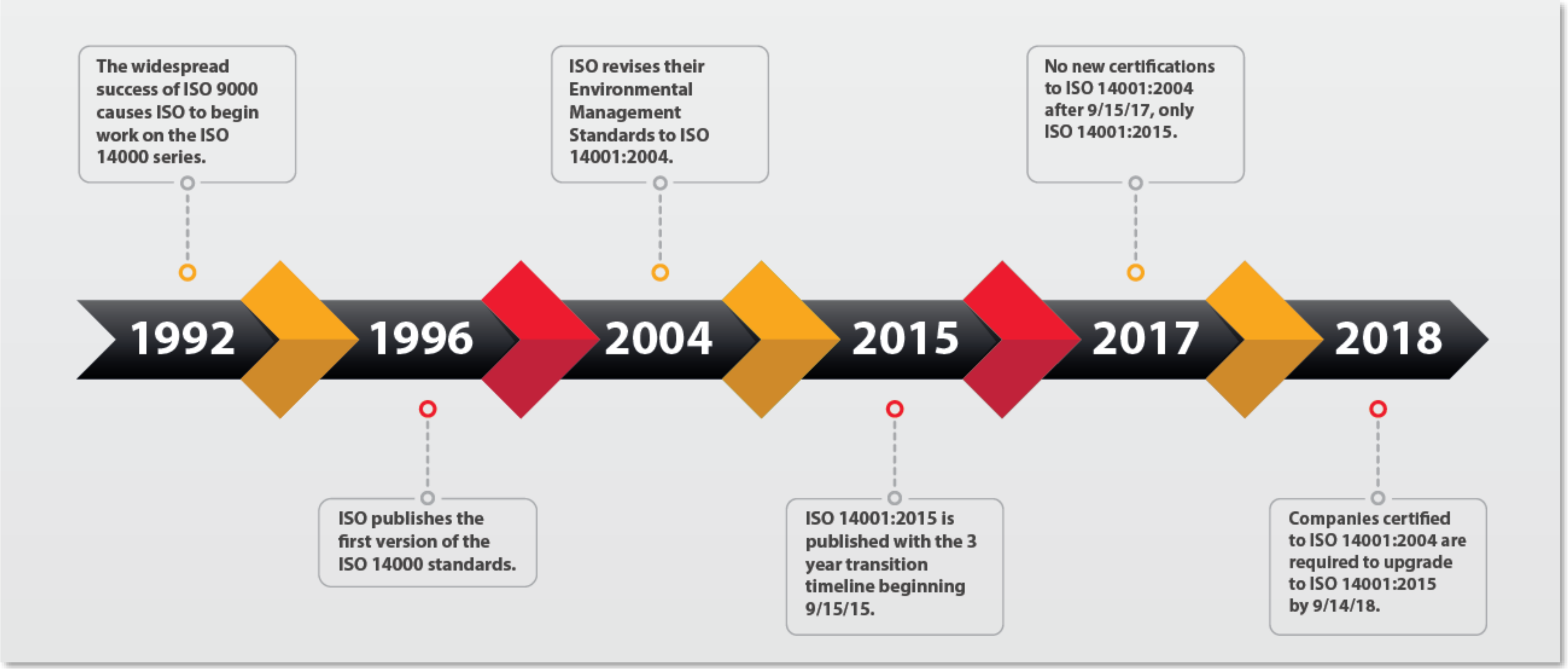
CPNI
Customer Proprietary
Network Information

CPNI

ISO 27001

ISO 9001

Certifications Evolve and Change



1992: The widespread success of ISO 9000 causes ISO to begin work on the ISO 14000 series.

1996: ISO publishes the first version of the ISO 14000 standards.

2004: ISO revises their Environmental Management Standards to ISO 14001:2004.

2015: ISO 14001:2015 is published with the 3 year transition timeline beginning 9/15/15.

2017: No new certifications to ISO 14001:2004 after 9/15/17, only ISO 14001:2015.

2018: Companies certified to ISO 14001:2004 are required to upgrade to ISO 14001:2015 by 9/14/18.

Evolution of ISO Standards

Certifications Are A Process

Initial Certification

Refresh Certification

Certification Change

Certifications Are A Process

Initial Certification

Refresh Certification

Certification Change

Your Vendor Needs A Continous Process For Maintaining and Adding Certifications

Verify Vendors' Security as a Service

Ask About Their Security Department

- Who leads it?
- What is their expertise?
- How many people?
- What tasks do they do?
- Where are they located?

Ask About Their Security Department

- Who leads it?
- What is their expertise?
- How many people?
- What tasks do they do?
- Where are they located?

EXAMPLE:

Mike McAlpen, CISSP, CISM, CSP
U.S. Strategic Infrastructure FBI (InfraGard) Healthcare Sector Chief

American Bar Association, Information Security Law Committee

Stanford Research Institute/DHS ITTC Cyber Defense Initiative

Partner, California State Regional Cyber Defense and Security Intelligence Center

ISSA Past Officer and Board Member

Secureworld Silicon Valley CISO Leadership Council

Past Multi-Term SF Chapter President of the ITIL U.S. IT Service Management Forum (ITSMF)

Past S.F. Chapter President and Executive Board member, National SIM CIO Organization

Ask To See Their Security Standards

- Get the documentation
- Understand what their standards are based on
- Look for the continuing process
- Who has access to data? (employees, contractors, third parties)
- How are their data centers secured?

Ask About Security Services to Customer

- Are they monitoring logins?
- Are they monitoring calling activity?
- What’s their pro-active response policy?
- Ask for a specific example of pro-active response
- How do they prevent security breaches?
- How often are they releasing security updates?

Ask About Penetration Testing

- Do they do it?
- How often?
- Who does it?
- What’s the surface area? (data centers, clients, more)

Ask For External Audits

- Most certifications require one
- Ask for audits specific to your clients’ certification needs
- Audits can be good verification even without certification needs
- Check how recent the audit is

In Conclusion

01 Cost of Failed Security

02 Security Is Not a Wall

03 Security As A Service

04 What Makes Up SaaS?

05 Certifications As A Service

06 Getting Good SaaS

07 Questions?

Questions

Overwhelmed? Need Help?

webinar@vertical.com

vertical
COMMUNICATIONS