From Cyber Security to Cyber Resilience: 5 Steps

Todd Begerow, Eastern Territory Manager
DNV GL Business Assurance, North America

Paige Needling, Information Security Sector Manager
DNV GL Business Assurance, North America

DNV GL –Your global business assurance partner

Position

One of the world's leading certification bodies

People

2,000 highly skilled specialized employees

10,000

Food and beverage companies partner with us to ensure safety and sustainability of their operations and supply chain

Partnership

with more than 70,000 customers in 187 countries

80,000

Management system (ISO 9001, 14001, 18001, etc.) certificates issued under more than 80 accreditations

2,400

Healthcare organizations trust us to help them improve quality and patient safety

DNV GL - Global reach – local competence

DNV GL's core competence is to identify, assess, and advise on how to effectively manage risk. Our independence and integrity are out main strengths. We have a global presence and a network of over 350 offices in 100 different countries.

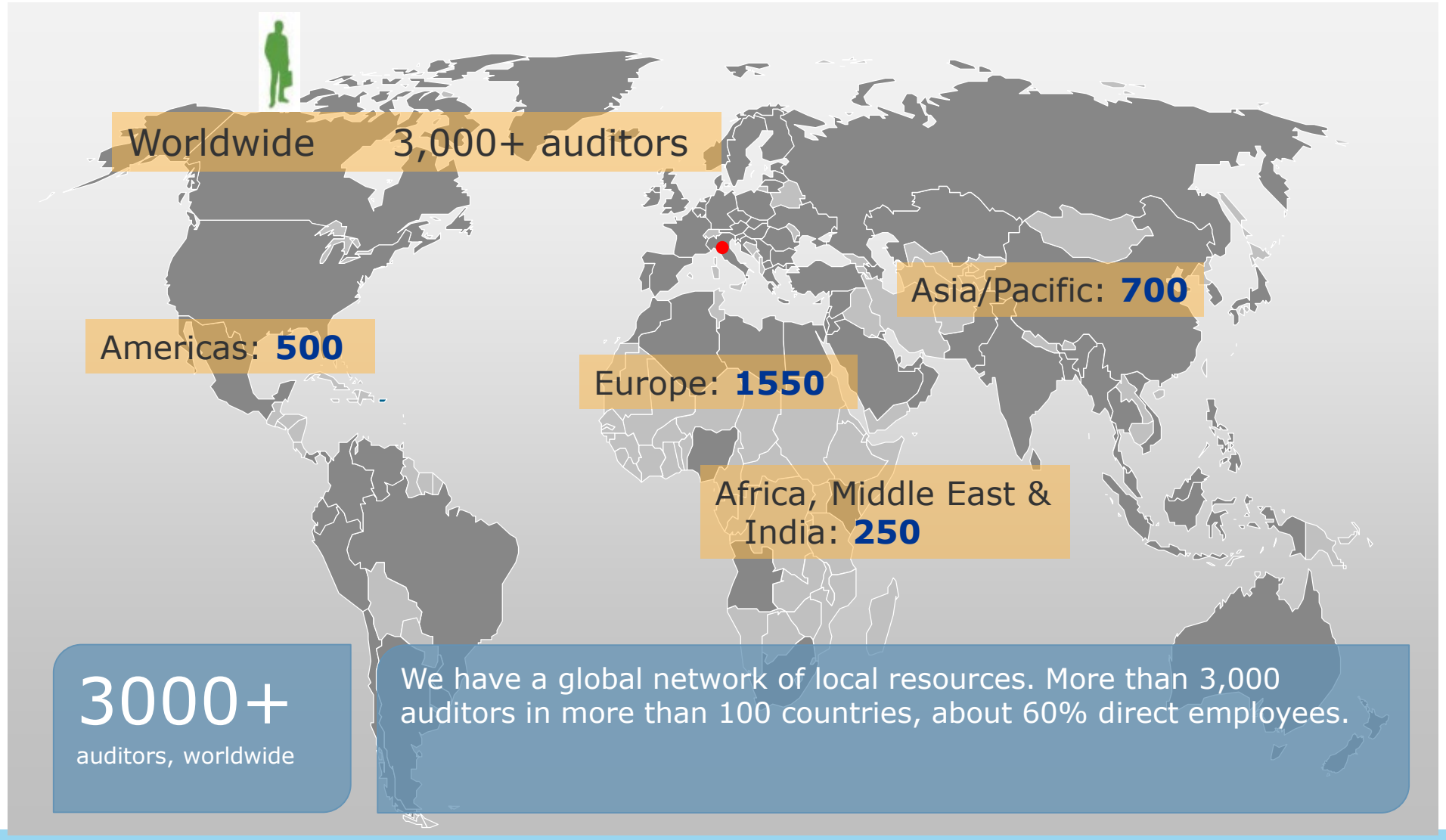
Our Purpose
To safeguard life, property, and the environment

Our Vision
Global impact for a safe and sustainable future

Our Values
- We build trust and confidence
- We never compromise on quality or integrity
- We are committed to teamwork and innovation
- We care for our customers and each other
- We embrace change and deliver results

Founded Since 1864	Oslo Head office	100	12,500
150+	350		
years	offices	countries	employees

Global Reach – Local Competence

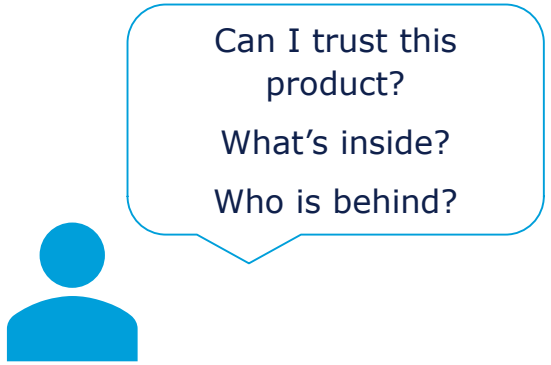


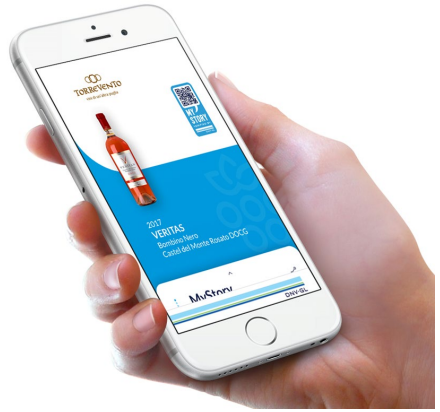
Digital Assurance and Transformation

- Blockchain Solutions – show origin, quality and social/environmental/ethical integrity of product to consumers displaying facts verified by DNV GL and immutably stored on VeChain platform.

MyStory

  - Since 2018, DNV GL's certificates are stored in a private BlockChain to improve security and transparency
- Virtual Auditing and Witness Assessments (sit by the pool while you participate in the audit)





CYBER RESILIENCY

New Rules. New Tools.

New Rule

However secure or vulnerable you think your information is, the truth is . . .

You've been hacked. Get over it.

Tipping Point

Breaches are so commonplace that success is now defined by the speed of recovery not the absence of compromise. It's a new ballgame.

	1990's – Early 2000's	Early 2000's - Onward
		
MINDSET	We're smarter and have more tech than the bad guys; an up-armored network protects us	We're outnumbered and behind the tech curve; data, devices and threats are everywhere
RESPONSIBILITY	IT department	Everyone
FOCAL POINT	Network edges	360^0
NEXT SCARY THING	Bots (controlled by bad guys)	AI (controlling itself)

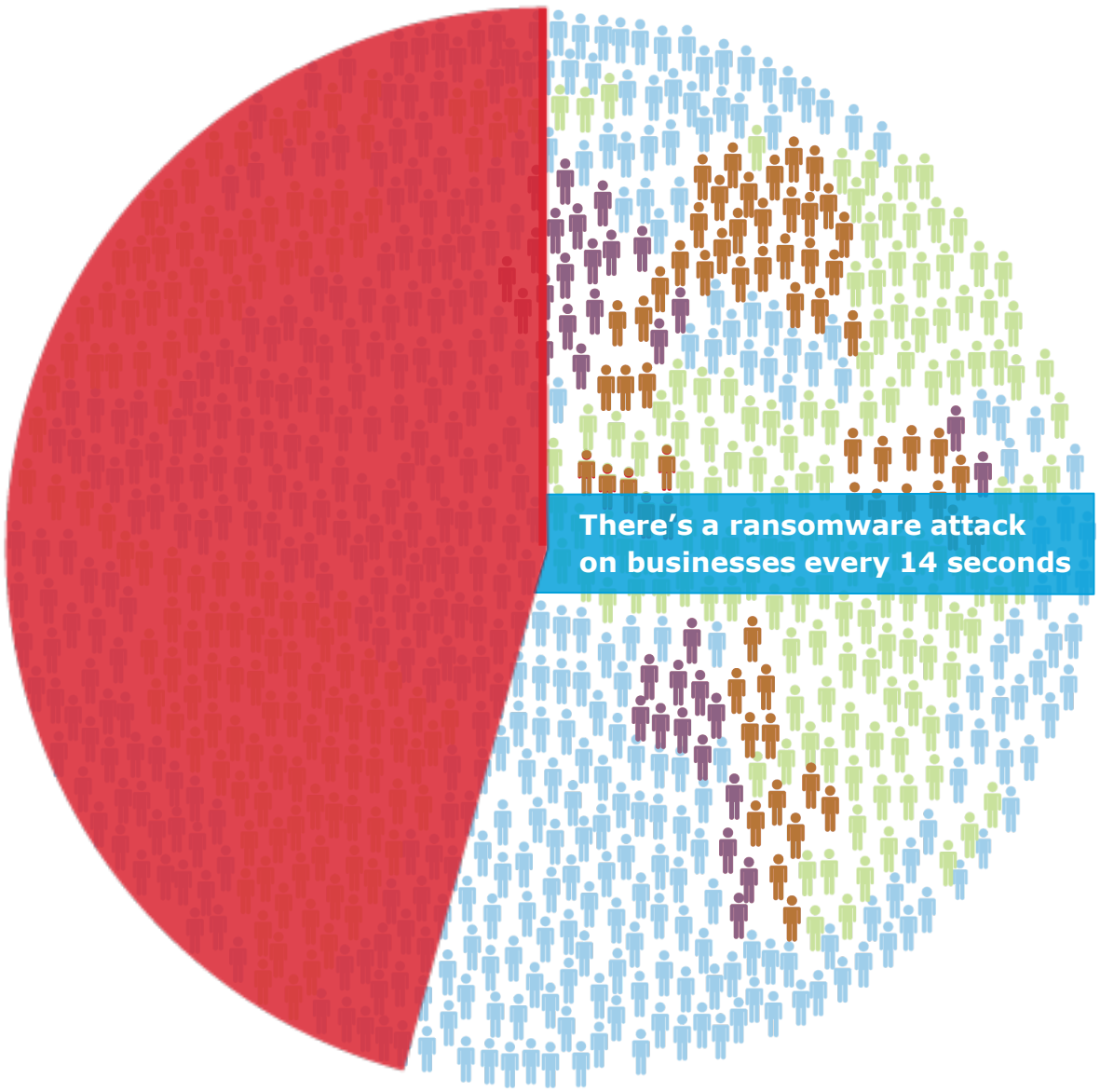
How did it get this way?

- Ubiquity of devices / mobile access
- Explosion in information sources
- Consumer tech drives business tech (users more casual)
- Pervasiveness of threats
- Dark web
- Human nature

AND FINALLY . . .

Cybercrime pays. Worldwide cost: $5.2 trillion annually.

Accenture, Securing the Digital Economy: Reinventing the Internet for Trust, 2019



21st Century Cyber Attacks

(CSO Online 12/18)

3 BILLION Yahoo
Almost half the world population

500 MILLION Marriott

145 MILLION eBay

135 MILLION Heartland

110 MILLION Target

57 MILLION Uber

2019 Forecast

80 Percent of U.S. Businesses Expect a Critical Breach in 2019

A primary cause of these risks was found to be complex, misaligned organizations with a lack of security connectivity, scalability and agility, and too few qualified people to manage security systems.

CRI (Cyber Risk Index) survey conducted by Trend Micro and The Ponemon Institute, Feb. 12, 2019

And earlier this month . . .

Security Discover, March 7, 2019

One of those e-marketing databases.

You never even know your name is on it.

Until it’s hacked.

Where's the leak?

A study using a sample of 419 companies in 13 countries and regions:

47% Malicious / criminal attack

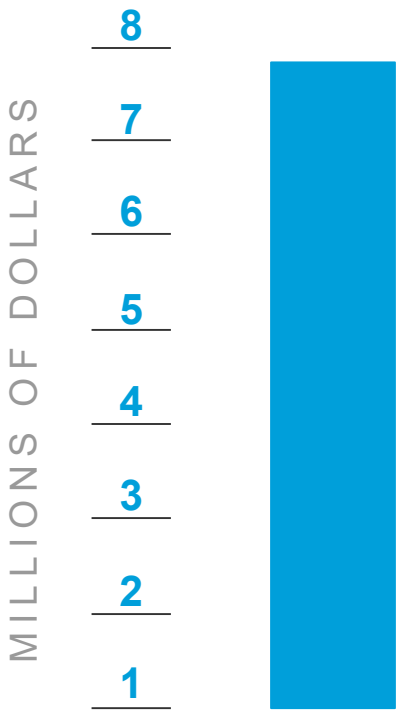
25% Negligent employees / contractors

28% System / IT malfunction

Ponemon Institute and IBM Security, 2017 Cost of Data Breach Study: Global Overview (Jun. 2017)

Cost of data breaches

Average cost in the US:



$7.91 million

A few whoppers:

Uber: **$150 million**

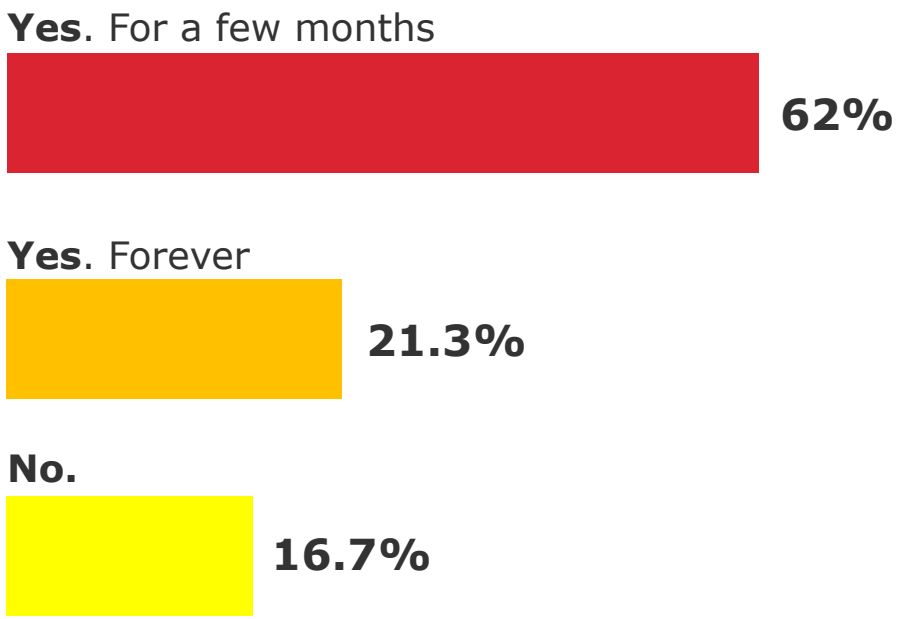
Anthem: **$131 million**

Yahoo: **$85 million**

Ponemon Institute and IBM Security, 2018 Cost of Data Breach Study: Global Overview (Jun. 2017)

Consumer impact

Will you **stop spending** with a brand after a hack. If so, for how long?



Threat Post

On the security horizon: More clouds

ZDNet

Cloud vulnerabilities are being ignored by the enterprise

Is there anything about putting your private information **in a cloud** that sounds secure?

And rising pressure

- SEC regulations
  - Cyber Unit formed 2017
- Laws being enacted, state by state
- Compliance demands (e.g., supply chain requiring ISO 27001)

> we expect companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences

SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Feb. 26, 2018

All talk?

only **14%** say board members understand cyber security risks

even though **90%** say they talk about it regularly

A study by the National Association of Corporate Directors, LEXOLOGY, Feb. 12, 2019

New Tools

Cyber resilience.

Anticipate vs. defend. Absorb the effects of a breach, survive and even grow because of it.

Resilience

Resilience is a healthy information ecosystem within an aware organization.

Able to:

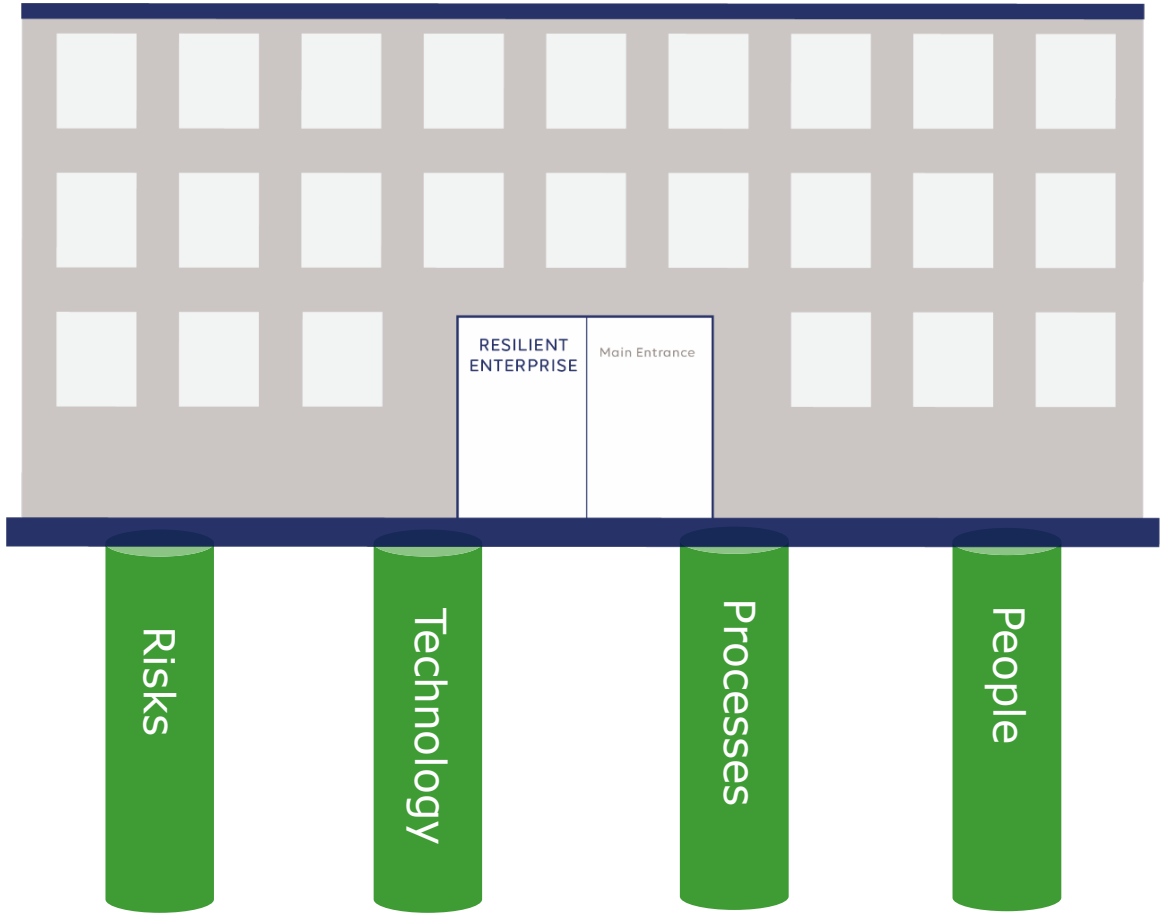
- Resist attacks and prevent leaks.
- Mount fast and efficient response to breaches.
- Restore – if necessary – normal business operations.
- Minimize (or eliminate) harm to customers, employees, suppliers . . . and thereby avoid damage to revenue, stock price and brand reputation.
- Swiftly and transparently address harm / damage to stakeholders should it occur.
- IMPROVE. Restore forward . . . not to where you were.

How does resiliency fail?

- **Failure in Recognition**: Not recognizing the problem, its symptoms or causes and differentiating between the two, not recognizing the scope of the problem for what it is and what is is likely to be or what is could be now, or in a couple of hours time.
- **Failure in Interpretation**: Not interpreting correctly what should have been recognized, analyzed, or correlated with threat intelligence, reality, or conflicting signals.
- **Failure in Decision Making**: There are decisions that were not taken, the wrong decisions that were taken, decisions taken for the wrong reasons, at the wrong times, and so on.
- **Failure in Action**: Even after decision are taken there are often failures attributed to their 'actionability' – so if the decisions were actionable, were they actioned fully correctly, in a timely fashion.

Pillars of Cyber Resiliency

The entire organization is part of the problem, and part of the cure.



Risks

- Understand your organization in it’s full business context
- Determine what is valuable and the calculate ‘pain’ of losing it
- Perform risk assessments against those things
- Compare vulnerability with liability (are you ‘covered’?)
- Do you have the necessary financial commitment?

People

- Educate your employees about cyber security
- Test your employees frequently on cyber security
- Provide information they can use at home and at work
- Provide information on security initiatives that they can share outside of the company

People

- **CISO**
  - Educate top management including Board
  - Drive strategic understanding; instill a culture of shared cyber-risk ownership
  - Identify key tech investments and talent
- **Chief Compliance / Risk Officer**
  - Provide guidelines and metrics to assess program's operational readiness and ability to respond
  - Risk analysis and assessment to identify deficiencies
- **CIO**
  - Should be seen as helping the CISO not driving the cybersecurity program
  - Work to ensure security is embedded from the beginning

Processes

- Robust incident response plan. Have one. Test it. Often.
- Budget: The scourge of “miscellaneous” costs
- Change management

Technology

- Defense in depth
- Anti virus malware
- Firewall
- VPN
- Data loss prevention
- Intrusion detection / preventions
- NAC
- SOC
- Biometrics (face, voice)
- Multifactor authentication
- AI (loop and quarantine)

Technology: 10,000 castles

Think inside and outside the box.

> The human 'perimeter' again and again appears to be the weakest link

Analysis of factors causing Anthem BC/BS breach
Bankinfosecurity.com, Jan. 10, 2017

In summary

- **Achieve True Visibility Across Your Entire Environment**

  You can't protect what you can't see. The first step to cyber-resilience is to obtain a big picture view of your enterprise in terms of all the assets – devices, users, and applications – connected into your environment, their breach risk, and the ability to drill down into details as needed.

- **Elevate Cyber-Resilience to Be a Board-Level Issue**

  There is an urgent need to recognize the profound risk of being breached and its far-reaching consequences for the organization, meaning that the responsibility for managing it sits at the board level. Educate your board of directors about breach risk and cyber-resilience and get their buy-in that your overall objective is to reduce breach risk by improving cyber-resilience.

- **Hire and Retain Top Talent**

  Tackling organizational issues, such as a shortage of security talent, to support operational and technical activities is a key issue that can keep CISOs challenged.

- **Develop a Laser-Focus on Security Fundamentals**

  Organizations cannot protect themselves at all times from the myriad of potential attacks through multiple channels. So, putting in place structures, technologies, and processes to build cyber-resilience are critical to operating effectively in today's hyper-connected world.

- **Get Proactive to Avoid Breaches**

  In the current sophisticated threat environment, traditional security tactics, which are mostly reactive blocking and remediation, are inadequate.

Cyber Resilience – Final Words

It's not another app, device or magic purpose. It's a unifying game plan for all of your security efforts. Know your risks. Know your responses. Know it works.

Become Resilient!

Polling Questions

1. Would you like guidance/assistance in creating or implementing an ISMS?

   Yes

   No

   I don’t know

2. Would you like assistance with ISMS Training?

   Yes

   No

   I don’t know

Contact Us

Paige Needling, Information Security System Sector Manager
Todd Begerow, Eastern Territory Manager
DNV GL Business Assurance, North America
ContactUs@dnvgl.com
(877) 368-3530
www.dnvgl.us/CyberResilience

Resources: