

# KEEPING INDEPENDENTS AHEAD OF THE CYBER THREAT

Mario Chiock, CISSP, CISM, CISA

Tweeter: @chiock



# AGENDA

- What do Oil & Data have in common ?
- Sample of Attacks in the Oil & Gas
- Cyber Threat – Statistics
- Technology alone is not the solution
- Cyber-security is the responsibility of everyone
- Cyber Threat – Essentials
- Takeaways



# WHAT DO OIL & DATA HAVE IN COMMON ?



# WHEN SPILLED ... BOTH CREATE A BIG MESS



## DATA Spilled on the internet





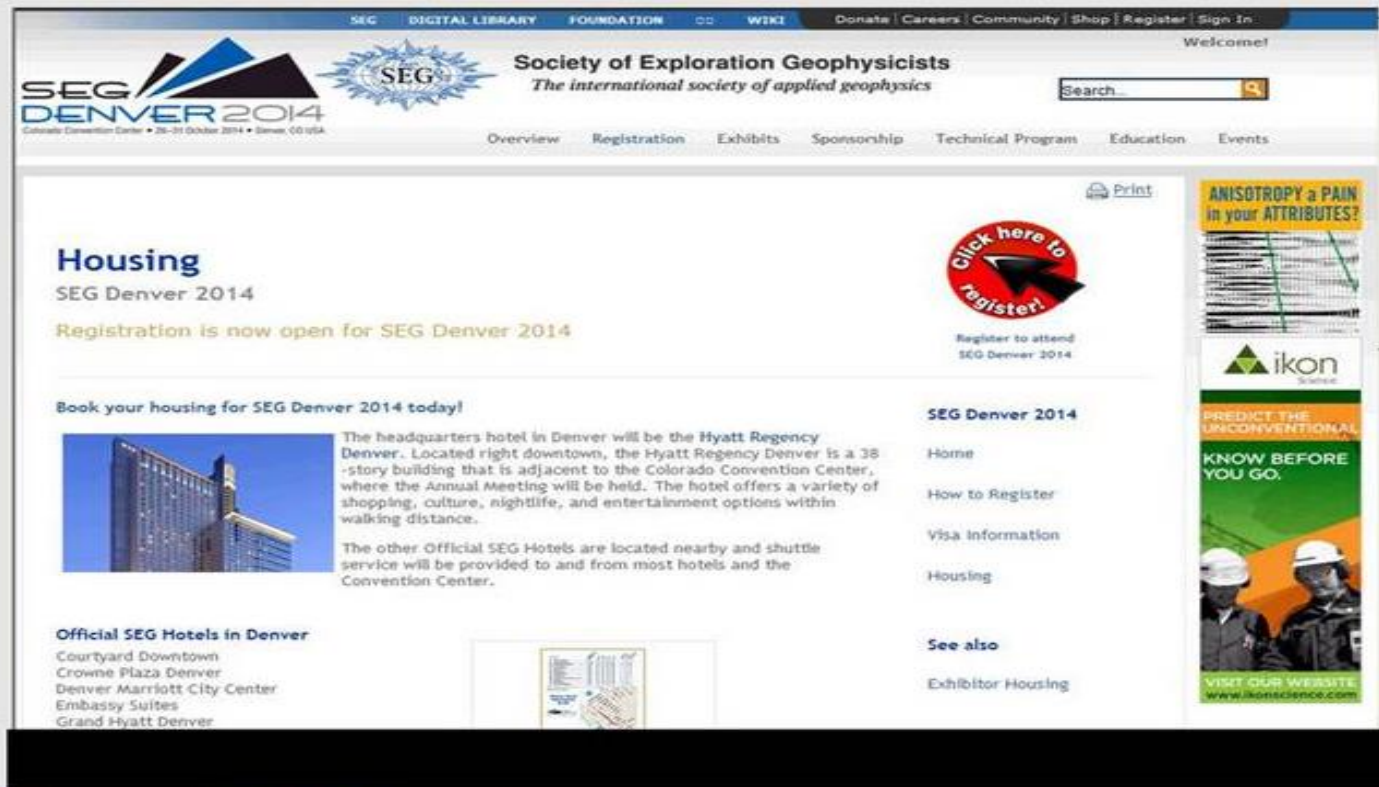
# SOCIETY OF EXPLORATION GEOLOGIST



*A fellow Houston InfraGard member in the energy sector shared the following information:*

It looks like some unknown actors have managed to compromise [www.seg.org/amhousing](http://www.seg.org/amhousing). SEG is a perfect target if your ultimate goal is the energy sector. We already had 20 of our folks receive a phishing email pointing that to that link. The phishing email header also contains the domain [exacttarget.com](http://exacttarget.com).

## SCREENSHOTS



Phishing directed users to :  
[www.seg.org/amhousing](http://www.seg.org/amhousing) Page

This page redirected to a  
Page that had:

Nuclear Exploit Kit  
&

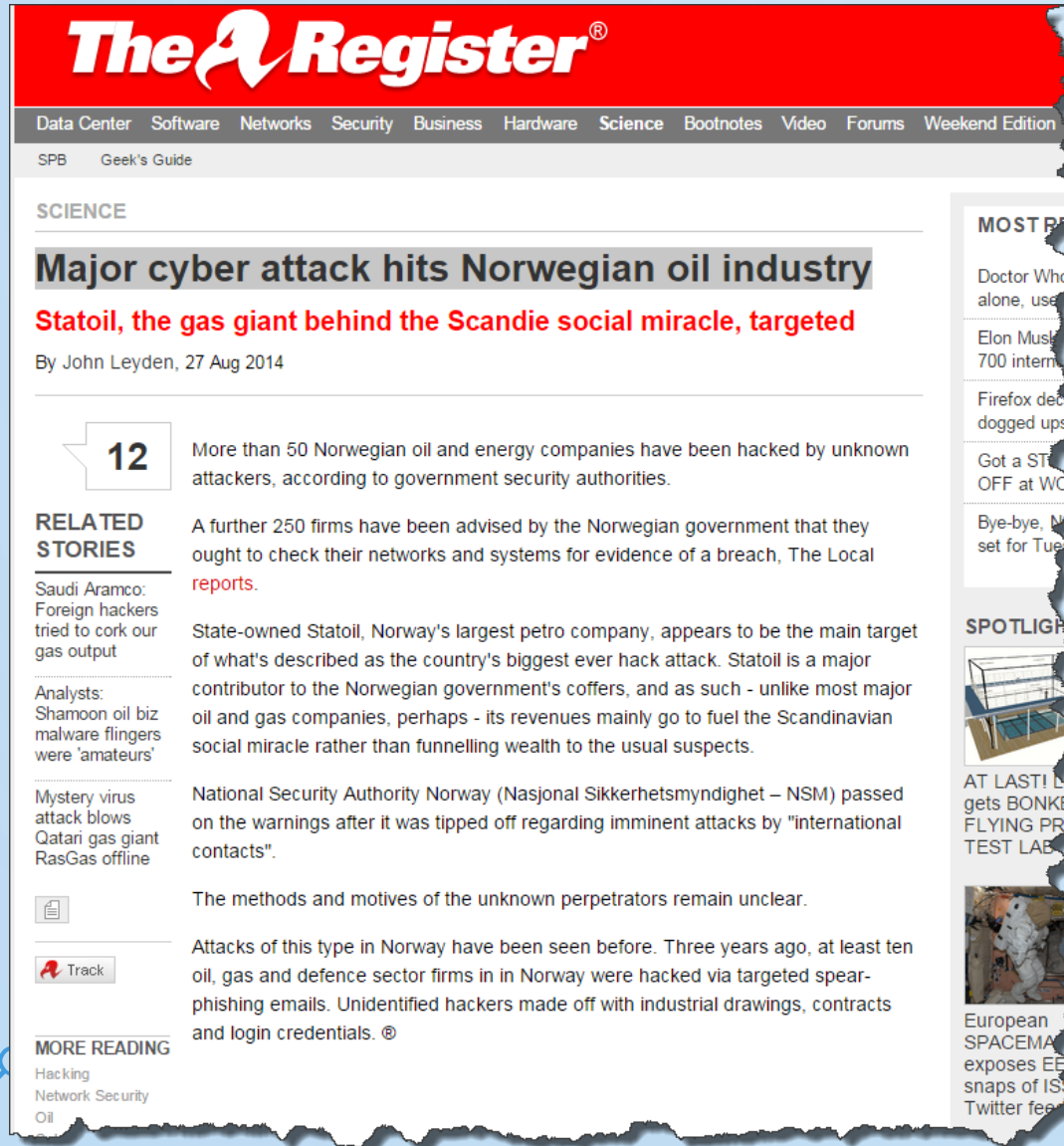
RIG Exploit kit

Taking control of the machine of the  
users clicking the link

Schlumberger

# MAJOR CYBER ATTACK HITS NORWEGIAN OIL INDUSTRY

[http://www.theregister.co.uk/2014/08/27/norwegian\\_oil\\_hack\\_campaign/](http://www.theregister.co.uk/2014/08/27/norwegian_oil_hack_campaign/)



**The Register®**

Data Center Software Networks Security Business Hardware Science Bootnotes Video Forums Weekend Edition

SPB Geek's Guide

**SCIENCE**

## Major cyber attack hits Norwegian oil industry

**Statoil, the gas giant behind the Scandic social miracle, targeted**

By John Leyden, 27 Aug 2014

**12** More than 50 Norwegian oil and energy companies have been hacked by unknown attackers, according to government security authorities.

**RELATED STORIES**

Saudi Aramco: Foreign hackers tried to cork our gas output

Analysts: Shamoon oil biz malware flingers were 'amateurs'

Mystery virus attack blows Qatari gas giant RasGas offline

A further 250 firms have been advised by the Norwegian government that they ought to check their networks and systems for evidence of a breach, The Local reports.

State-owned Statoil, Norway's largest petro company, appears to be the main target of what's described as the country's biggest ever hack attack. Statoil is a major contributor to the Norwegian government's coffers, and as such - unlike most major oil and gas companies, perhaps - its revenues mainly go to fuel the Scandinavian social miracle rather than funnelling wealth to the usual suspects.

National Security Authority Norway (Nasjonal Sikkerhetsmyndighet – NSM) passed on the warnings after it was tipped off regarding imminent attacks by "international contacts".

The methods and motives of the unknown perpetrators remain unclear.

Attacks of this type in Norway have been seen before. Three years ago, at least ten oil, gas and defence sector firms in Norway were hacked via targeted spear-phishing emails. Unidentified hackers made off with industrial drawings, contracts and login credentials. ©

**MORE READING**

Hacking  
Network Security  
Oil

**MOST POPULAR**

Doctor Who alone, use

Elon Musk 700 intern

Firefox de... dogged upst

Got a ST... OFF at WO

Bye-bye, M... set for Tue

**SPOTLIGHT**

AT LAST! L... gets BONKE... FLYING PRI... TEST LAB

European SPACEMA... exposes EE... snaps of ISS... Twitter fee

*Approximately 300 oil and energy companies in Norway have been hit by one of the biggest cyber-attacks ever to have happened in the country. “Spear phishing attacks – increasingly through the compromised systems of small suppliers to large companies– is an increasingly interesting attack vector for criminals attempting to steal valuable information and IP”.*

# SAUDI ARAMCO - SHAMOON



- +30,000 machines
- Insider Exploiting privilege account
- Use of def
- Use of sha

```

1. mon 29th aug, good day, SHN/AMOO/lib/pr/~reversed
2.
3. We think it's funny and weird that there are no news coming out from Saudi Aramco regarding Saturday's night. well, we expect that but
  just to make it more clear and prove that we're done with we promised, just read the following facts -valuable ones- about the
  company's systems:
4.
5. - internet service routers are three and their info as follows:
   ss-ar-cr-bl
   ss-ar-bk-bl
   ss-ar-st-bl
   - Khalid A. Al-Falih, CEO, email info as follows:
     Khalid.falih@aramco.com      password:kal@ram@sa1960
12.
13. - security appliances used:
14. Cisco ASA # McAfee # FireEye : default passwords for all!!!!!!!!!!!!
15.
16. We think and truly believe that our mission is done and we need no more time to waste. I guess it's time for SA to yell and release
    something to the public. however, silence is no solution.
17.
18. I hope you enjoyed that. and wait our final paste regarding SHN/AMOO/lib/pr/~
19.
20. angry internet lovers
21. #SH
```





# OTHER CYBER ATTACK TO OIL & GAS



<http://www.houstonchronicle.com/business/energy/article/Malware-on-oil-rig-computers-raises-security-fears-4301773.php>

**HOUSTON CHRONICLE**  
**ENERGY**

**WORLD** **SPORTS** **BUSINESS** **OPINION** **ARTS & ENTERTAINMENT** **LIFESTYLE**

Real Estate Personal Finance Top Workplaces

## Malware on oil rig computers raises security fears



31 August 2012 Last updated at 05:10 ET

Share

### Computer virus hits second energy firm

Computer systems at energy firm RasGas have been taken offline by a computer virus only days after a similar attack on oil giant Aramco.

The attacks come as security experts warn of efforts by malicious hackers to target the oil and energy industry.

The attack forced the Qatar-based RasGas firm to shut down its website and email systems.

RasGas, one of the world's largest producers of liquid petroleum gas, said production was not hit by the attack.

The company said it spotted the "unknown virus" earlier this week and took desktop computers, email and web servers offline as it cleaned up.

The report comes only days after Saudi Arabia's Aramco revealed it had completed a clean-up operation after a virus knocked out 30,000 of its computers. The cyber-assault on Aramco also only hit desktop computers rather than operational plant and machinery.

Both attacks come in the wake of alerts issued by security firms about a virus called "Shamoon" or "Disstrack" that specifically targets companies in the oil and energy sectors.



Oil and energy firms are being targeted by a destructive virus say security researchers

**Related Stories**

- Oil giant recovers from net virus
- New virus targets energy sector
- US probes power plant 'backdoor'

**NEWS**

## Exxon, Shell, BP hacked in Night Dragon attacks

Thursday 24 February 2011 09:19

Share

Exxon Mobil, Royal Dutch Shell and BP were among the oil companies targeted by hackers working through internet servers in China, say US reports.

IT security firm McAfee reported on 10 February that the attacks had resulted in the loss of project-financing information relating to oil and gas field bids and operations.



McAfee said the attacks started in November 2009, but it did not identify the oil companies that were affected.

"We have identified the tools, techniques, and network activities used in these continuing attacks, which we have dubbed "Night Dragon," as originating primarily in China," McAfee said.

The hacked companies also include Marathon Oil, ConocoPhillips and Baker Hughes, according to Bloomberg, citing company sources and investigators who asked not to be identified because of the confidential nature of the matter.

In some of the cases, hackers had undetected access to company networks for more than a year, according to Greg Hoglund, chief executive officer of security firm HBGary, which investigated some of the security breaches at oil companies.

Legal information, information on deals and financial information are all things that appear to be getting targeted, he said, describing the attacks as industrial espionage.

<http://www.computerweekly.com/news/1280095257/Exxon-Shell-BP-hacked-in-Night-Dragon-attacks>

# Schlumberger



# HACKERS BREAK INTO CORPORATE SYSTEMS THROUGH VENDING MACHINES AND ONLINE RESTAURANT MENUS



<http://www.allgov.com/news/unusual-news/hackers-break-into-corporate-systems-through-vending-machines-and-online-restaurant-menus-140409?news=852874>

## Hackers Break into Corporate Systems through Vending Machines and Online Restaurant Menus



(AP photo)

With firewalls ever more difficult to breach, hackers have found other ways to sneak into protected computer systems, even those involving restaurant menus and soda machines.

When an employee uses his or her company computer to order food through an online menu, they can open up a cyber door for intruders to slip through and gain access to the local network of servers.

That's what happened to one unidentified oil company, *The New York Times* reported, when hackers attached malware to an online menu belonging to a Chinese restaurant frequented by the oil firm's employees. Simply browsing the menu resulted in the malicious code downloading into the user's computer and on to others at the corporation.

Vending machines set up in company break rooms also can provide a backdoor into a supposedly secure network. Many such machines contain minicomputers that allow the vendor to remotely check on the supplies of soft drinks. But the same system can be utilized by hackers to infiltrate the computers of the company hosting the vending machines.

Printers, thermostats and videoconferencing equipment can also be vulnerable to intruders.

In other cases, hackers break in through a third-party's computer system, such as those providing heating and air conditioning at an office. This happened to retailer Target, which had its payment card system breached, potentially costing the company up to \$420 million.

Top Stories

Unusual News

Where is the Money Going?

Controversies

U.S. and the World

Appointments and Resignations

Latest News

When Parents Die, Private

Military Judge Orders Release of  
Torture at Secret Prison

IRS Paid Bonuses to 1,100

# Schlumberger

# PHISHING STILL HOOKS ENERGY WORKERS

<http://fuelfix.com/blog/2013/12/22/phishing-still-hooks-energy-workers/>



[Home](#) [Oil Field](#) [Pipelines](#) [Refining](#) [Power](#) [Washington](#) [Voices](#) [Jobs & Career Advice](#)

## Phishing still hooks energy workers

Posted on December 22, 2013 at 6:30 am by [Zain Shauk](#) in [Premium](#), [Safety/Security](#)

HOUSTON — The largest energy companies want their workers to stop clicking on links to cute cat photos.

Such emailed links are among the leading ways that hackers gain access to energy company systems — a trick known as phishing, with the potential for breaches that could lead to huge thefts of data, or even physical damage.

Phishing attackers try to get computer users to click on a link or download an attachment in an email that allows hackers to enter their systems.

In their latest counterattack, Schlumberger, Shell and other major players in the energy sector have been sending their employees fake phishing emails.

Unfortunately for many companies, employees are easily coaxed into clicking on bad links, said Jim Hansen, executive vice president for PhishMe, which specializes in phishing risks.

"Something as foolish as silly pictures of cats," Hansen said. "You think it's not going to happen. It always happens

(Fotolia for Frances)



**Schlumberger**

# CYBER THREAT – STATISTICS



- 70% of Breaches are found by 3<sup>rd</sup> parties
  - Law Enforcement
  - Other investigations
  - Partner or customer
  - others
- 74% of Breaches where not detected in months
- 5% of Breaches were not detected over a year
- Method of attack
  - Phishing
  - Vishing
  - Malware
  - 3<sup>rd</sup> Party - Insider
- 85% of incidents successful in minutes
- Most Frequent Cause of Breaches:  
Negligence - 41%
- 50% data successfully exfiltrated in few hours

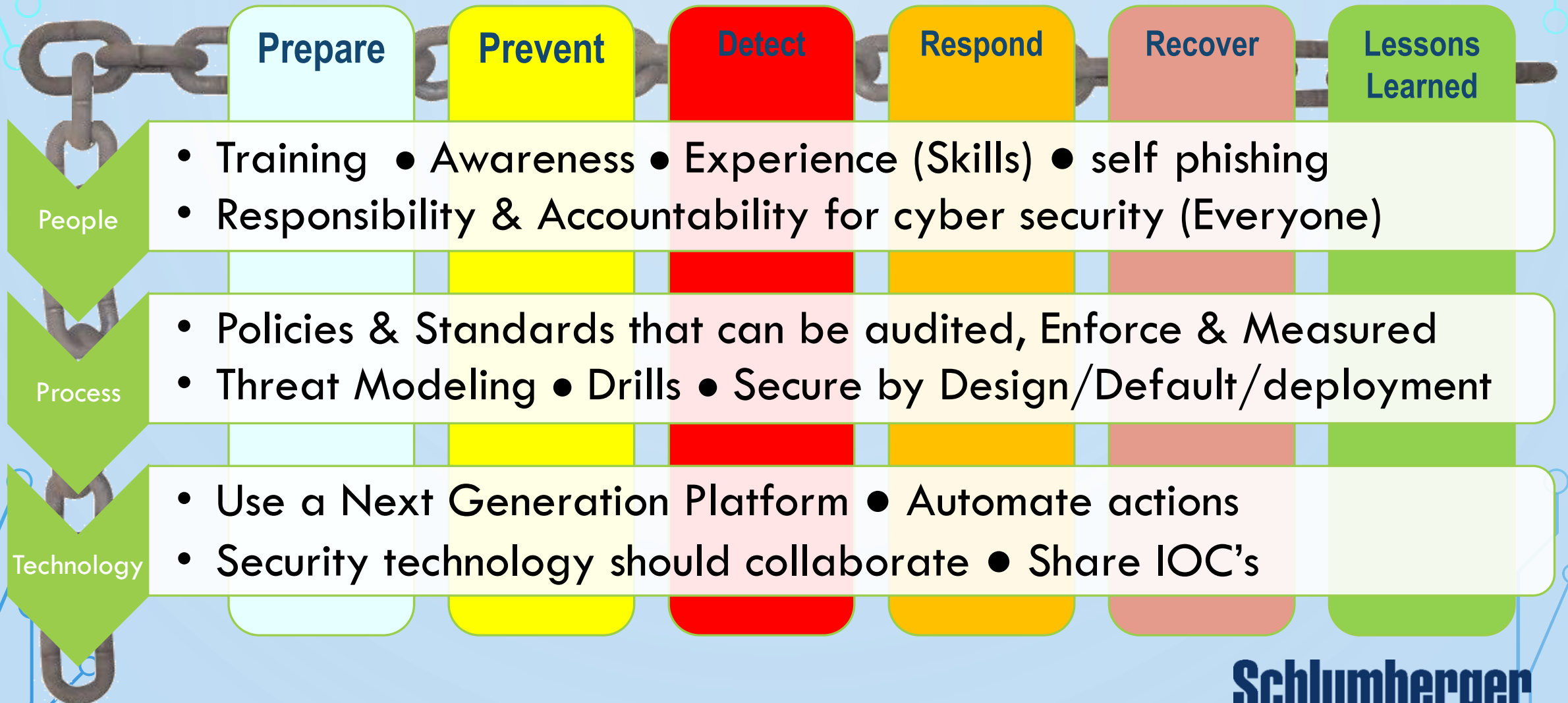
**Many companies been breach just don't know it yet**

Source: 2013 Verizon Data Breach Investigations Report & Ponemon Institute

**Schlumberger**



# TECHNOLOGY ALONE IS NOT THE SOLUTION



# CYBER SECURITY MUST BE ON EVERYONE'S AGENDA



Board  
CEO  
CFO

## Executives

What is the potential  
impact of a cyber  
breach-attack  
Mitigate Risk

## Information Technology

We manage the IT  
Infrastructure &  
Software  
We need to protect IT

## ALL

Employees  
&  
Contractors

## Business

We need to use the  
Data  
We need to use the  
Technology  
We need to protect the  
DATA and Technology

CIO  
Business Systems  
Helpdesk  
Data Centers  
IT Security  
IT Operations  
Networks  
Servers  
Desktops

Operations  
Marketing  
HR  
Legal  
HSE  
Supply Chain  
Operational Technology

**Schlumberger**

# CYBER THREAT - ESSENTIALS



## Information Sharing

ONG-ISAC

InfraGard

Engage with FBI – DHS

## Incident Response

Invest on Preparedness

Desktop exercise

Root Cause Analysis

**Concentrate in basic  
Cyber Hygiene**

## Executive Buy-In

Everyone Responsible & Accountable

Adopt the Safety Culture into Cyber-Security

IT & OT need to work together

## Build Cyber-Security Skill set

Training

Network with peers

Adopt Best Practices



# TAKEAWAYS

- Technology alone is not the solution
  - Information Sharing
  - Prepare for the worse
- Cyber-security is the responsibility of everyone
- Concentrate on Essentials & Cyber-security Hygiene
- Train your staff & build cyber-security skills



# USEFUL ORGANIZATIONS

- ONG-ISAC - <http://www.ongisac.org/>
- InfraGard – <https://www.infragard.org/>
- ISSA – <http://www.issa.org/>
- ISACA – <https://www.isaca.org>
- ICS-CERT
- US-CERT
- STOP-Think-Connect (<http://www.dhs.gov/stopthinkconnect>)
- NIST - <http://www.nist.gov/cyberframework/>