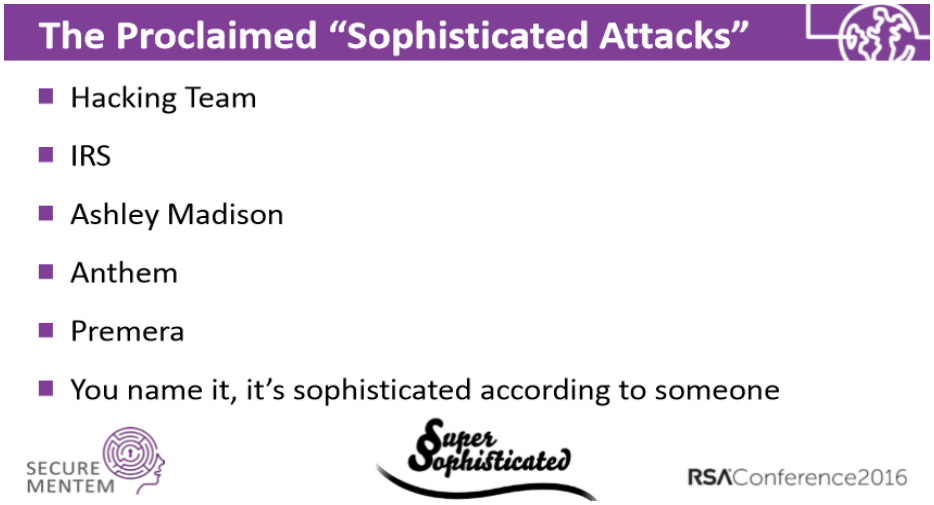
Cyber Attack Trends, Neoscope Shield Case Study, and CEO Perspectives

Author: Craig M Taylor, Chief Security Officer – Neoscope Technology Solutions
March 6th, 2016

This security whitepaper contains three main sections. First, we present detailed statistics on security breach trends and whether they are successful due to sophisticated attacks or simple bad security practices. Second, we outline the unique experiences of two clients – one Neoscope Shield client and one who is not (but should be). Finally, we provide current CEO perspectives on Cybersecurity program needs, practices, and the boardroom interactions and expectations they face.

1) Successful Cyber Attacks due to Bad Security not Sophisticated Attacks

2015 Security Breaches yield surprising insights into the nature and commonalities of successful attacks. Attackers were successful due to ***bad security rather than sophisticated actors and attacks***. Basic security is where the Neoscope Shield excels. It targets the weakest links in any security program – the people – and seeks to train and guide them while bolstering the technical controls that backstop those risks even when people make mistakes!



Trends in these Attacks

Passwords:

- *Hacking Team* used passw0rd
- Pass1234 was used in the *Ashley Madison* case
- A compromised administrator credential was present in *Anthem* breach

Flat Networks and no Detection Capacity:

- Flat networks present in the *Hacking Team* network led to easy data theft
- Improperly segmented networks at *Premera*
- Undetected attack at *Anthem* for 9 months despite massive data queries

Missing Risk Assessment Could have detected Critical Risk before Exploited:

- 'Get Transcript' website function at the *IRS* lacked a detection mechanisms leading to 700k fraudulent but successful recovery attempts by hackers
- SQL Injection attacks within *Ashley Madison* application, no network segmentation, and failure to delete accounts
- No Multi-factor authentication at any of these companies

Lack of Security Awareness Culture:

- Poor security awareness at *Premera*

Conclusions

Attacks are successful not because they are advanced or sophisticated, but because they are adaptive and persistent. Therefore, expect failure, be adaptive and persistent in your response, your training, and your technology, analyze your likely threats (risk assessment), determine the appropriate protection needed surrounding your critical data, and determine if you have Detection Deficit Disorder (DDD).

Recommendations

- People play a critical role in Prevention, Detection, and Reaction
- A strong security Culture prevents and detects incidents

2015 Verizon Data Breach Security Incidents by Industry:

Let's begin with the latest security incident breach statistics across industry from the 2015 Verizon Data Breach report (a global report summarizing ALL public and many private data breaches metrics that occurred in 2015 from over 100 global entities). Highlighted are two sectors – Financial Services (Client #1) and secondly, Professional Services (Client #2) for comparison purposes.

	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services (52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31–33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44–45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48–49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

Figure 2.
Security incidents by victim industry and organization size

Outside of the massive public sector breaches (50k), Financial Service clients (642) were the second most heavily targeted industry segment. Professional services are a distant 7th (347). Breaches are happening across all industries in ever increasing frequency with the lion's share being reported by government agencies in the public sector.

2) Case Study: Neoscope Shield Client vs. Non-Neoscope Shield Client

These case studies outline real-world events relating to two Neoscope clients. The first client is a medium sized financial services firm with over 500+ clients who uses the Neoscope Shield Managed Security Service Provider (MSSP) offering. The second client is a Professional Service Industry client who refused the Neoscope Shield MSSP offering despite our strong suggestion.

Case Study #1: Financial Services Firm Using the Neoscope Shield

A New England financial service firm was under attack. They were receiving phishing emails, virus attachments, and attacks on their website and turned to Neoscope to develop a defense-in-depth

security program to protect the critical financial information they had for 500+ clients. The Neoscope Shield was deployed and provided the following key benefits:

Technical Protections:

- **Quarterly Vulnerability assessments** of their Firewall and website identified misconfigurations (unnecessary open ports) in their firewall that were subsequently closed and a potential website vulnerability that could have led to defacement, or worse – hosting malware.
- **Advanced Malware Protection:** AV products today are less than 50% effective at identifying and preventing malware infections. Consequently, the Neoscope Shield bundles advanced malware protection via DNS in order to block emerging threats more quickly (in hours not days).

Administrative Protections:

- **Security Awareness Training** was given to their staff teaching them how to spot Phishing emails, social engineering attempts, the importance of picking strong passwords. Subsequent client reports showed staff members identifying Phishing emails and deleting them without incident.
- **Governance Policies:** In accordance with Massachusetts Data Privacy legislation (CMR 201 17), this accounting firm didn't have a Written Information Security Policy (WISP) and wasn't compliant with this privacy legislation. A WISP was implemented under the Neoscope Shield alongside other important governance policies including a Password Policy, Acceptable Use Policy, Information Handling Policy, and Security Awareness Training Policy.
- **Risk Assessment:** a formal risk assessment was performed by Neoscope. Physical, Administrative, and Technology risks were identified, prioritized, and mitigating controls developed and implemented. One risk identified was that all laptops containing privileged client data needed, and subsequently received, full-disk encryption because of the data they contained.
- **CSO Consulting:** few organizations in the small to medium sized marketplace can afford a competent, experienced CSO. This client benefits from their CSO consultant at Neoscope answering their critical security questions on nights, weekends, or during an audit.

Physical Protections:

- The risk assessment also identified physical protections needed at this accounting firm. They now are very diligent about locking up all sensitive client data and destroying (shredding) all paper materials no longer needed on a daily basis.

Through the risk assessment and related mitigating controls deployed this client has prepared itself for the myriad of threats they face in a highly targeted industry. In 2016 the IRS continues to reveal ever more financial records that were breached in 2015 (700,000 as of this writing). This client has put the necessary governance policies, security awareness training, and technology protections in place to protect itself. The Neoscope Shield bundle is not a guarantee against breach, and while this accounting firm has been repeatedly targeted by attackers as they operate in the 2nd most attacked industry, *they have yet to experience a security breach of their network and/or client data*. This client is miles ahead of their competitors in preparing for, preventing, and responding to any breach and remains well protected through policy, process, and technology protections under the Neoscope Shield.

Case Study #2: Professional Services Firm Not Using Neoscope Shield

On the other end of the spectrum of Neoscope clients is a client we have tried unsuccessfully to get onto the Neoscope Shield program that has subsequently experienced two Cryptolocker infections, a Remote Access Trojan compromise of a server, and numerous workstation outages, **all due to bad security**. *They lack a security awareness program, clear governance policies, and technology protections for their organization.*

This client operates in an industry vertical (professional services) that is much *less likely* to be targeted by attackers according to the Verizon Data Breach report. Specifically, they are 7th on the list.

Anatomy of their Attacks

In the most recent attack Neoscope responded to and remediated, a remote attacker who was successful in installing a Remote Access Trojan (RAT) on a server in their network by exploiting a known vulnerability on that server. The attacker then pivoted and expanded their attack by creating a local administrator account (which Neoscope monitoring immediately identified alerted us on). The attacker then installed a RAT for future command and control activities. Previous attacks on this client included staff clicking on emailed attachments causing Cryptolocker infections on two separate occasions. Fortunately, Neoscope's robust backup solution was able to return them to normal operations, preventing permanent damage to this firm.

Had this client deployed the Neoscope Shield, these security incidents might not have occurred. Here's why:

1) Our vulnerability assessment would have identified the vulnerability in their server on a port and protocol being passed through their firewall.
2) Our security awareness training would have given the two employees pause before they clicked on the Cryptolocker email attachment and infected their network and all the file shares they had access to.
3) A risk assessment would have identified the need to migrate all users from direct inbound access to the compromised server and onto a VPN solution
4) Our Risk Assessment would have identified opportunities to further strengthen their active directory password requirements potentially preventing success attacks.

This firm remains in a ***highly reactive stance***, taking their chances at recognizing and thwarting their next attack. As a consequence, and due to their inaction, they have experienced hours of down-time, costly security incident recovery costs, and tremendous risk to their reputation.

The next section of this whitepaper will move into Industry Trends at the CEO and board level of companies. At the 2016 RSA Security Conference, many speakers expressed the need to become proactive at all levels of a company but none more-so than at the CEO and Boardroom levels.

3) Cyber Security Trends Reported by Chief Executive Officers (CEO)

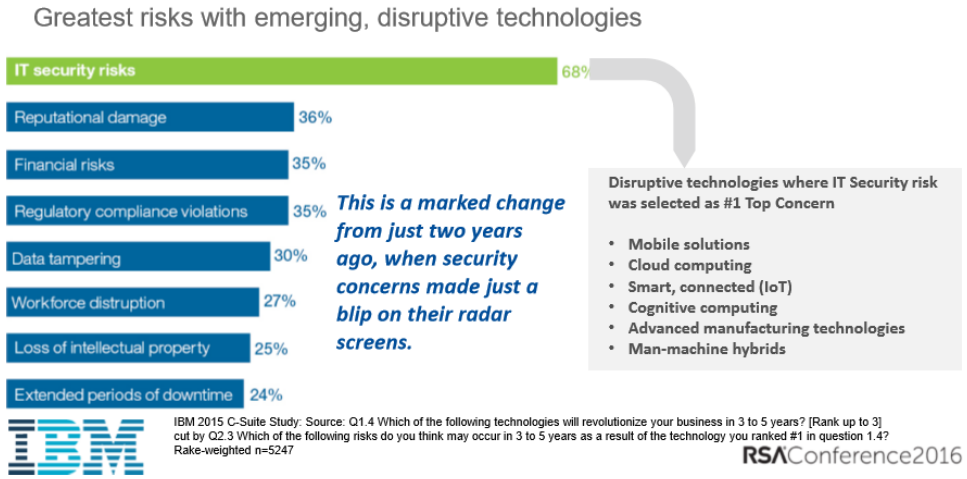
This 3rd section of the white paper summarizes trends in cybersecurity awareness at the CEO level across multiple industries as reported by IBM in a 2015 research project. These results were presented at the 2016 RSA Security Conference and are summarized below.

75% of C-Suite Think Security Program is Important

Clearly there has been a shift in corporate America over the last 2-3 years. Boards and C-Suite executives are painfully aware of the critical threats their companies face. This is reflected in the following slide which summarizes 691 C-level executives view on security programs (and components).

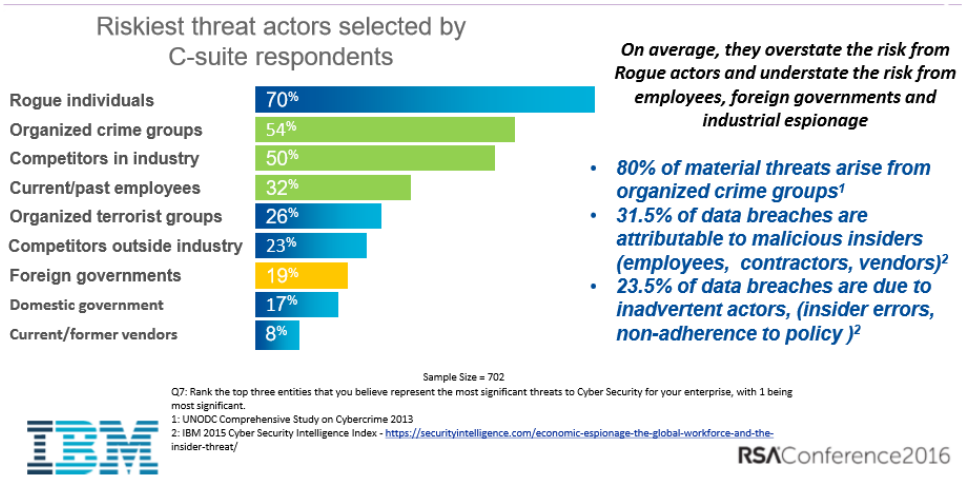
What are the greatest IT Security Risks Companies Face?

The top 3 risks identified by C-level executives include reputational damage (36%), Financial damage (35%), and Regulatory compliance violations (35%) the latter of which is most heavily regulated in the healthcare industry.



Common misconceptions on Risk Remain at the C-Suite Level

C-Level executives tend to overestimate the risk of rogue actors and underestimate the impact of organized crime groups.

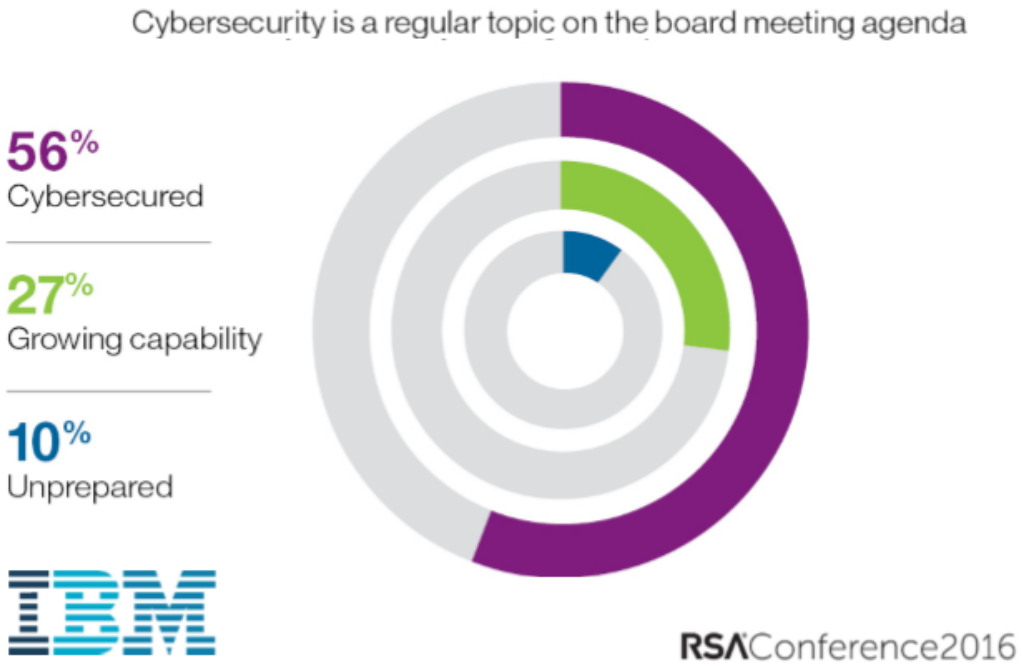


Chief Information Security Officer Trends

Many of the C-level executives polled by IBM identified plans in to establish or grow the capacity of a CISO within their organization. Until SMB's get large enough, a CISO or CSO consultant is a strong play to provide security program development and oversight for a burgeoning business in any industry.

Cybersecurity Transparency/Communication are Increasingly a Board Room Conversation

Board rooms are increasingly asking the question: "*What preparations are we making on Cyber-Security?*" and "*How prepared are we to prevent, detect, recover from, and revise our security program after a Cyber-security incident?*"



Overall White Paper Conclusions

Company CEO's today recognize the increasing importance of building a proactive Cyber-security program designed to address basic information security needs across governance policies, awareness training, and technology controls. Contrary to media portrayals of sophisticated attacks being inevitable, a proactive simplified approach to basic cyber security protections (Risk Assessment, Governance Policies, Technology Controls and Awareness Training) could have prevented many of the highly publicized attacks of 2015. The Neoscope Shield is designed to blend the most cost-effective, efficient, and time-sensitive training, policy guidance, and technology controls together and in so doing properly secure our client's critical information and systems for worry free success.

References:

IBM C-Suite Survey Report: http://www-03.ibm.com/security/ciso/

Verizon Data Breach Report: http://www.verizonenterprise.com/DBIR/2015/

Neoscope Shield Offering: https://www.neoscopeit.com/neoscope-shield