FAILURES OF THE SECURITY INDUSTRY: ACCOUNTABILITY AND ACTION PLAN

Amit Yoran
President, RSA

William Robertson
Assistant Professor
College of Computer and Information Science, Northeastern University

The information security industry is losing the cyberwar. Make that *cyberwars*. Plural. Black hat "hacktivists," organized crime syndicates, state-sponsored operatives, terrorists, and other threat actors attack computer systems and critical infrastructure on multiple fronts across the globe with seeming impunity. Motivations and objectives vary. The common thread is malicious intent. Backed by alarmingly sophisticated skills and deep resources, these 21st century intruders frequently succeed in attaining their objectives. But, it is not only the sophisticated that succeed. Often, perpetrators with more persistence than acumen are able to exploit weaknesses. Enterprises unwittingly provide broad attack surfaces with inadequately secured or completely vulnerable points of entry. Whether targets of adept cyber saboteurs and criminals or of their own lack of preparation and investment, victims of cyberattacks sustain damages that range from isolated annoyance to devastating, expansive…and expensive.

The adverse financial impact alone is staggering. Factor in how the relentless barrage of cybersecurity breaches weaken the security of sovereign nations, stifle innovation, lower consumer confidence and threaten public safety, and the magnitude of the problem is truly intimidating. Cybercrime hurts the global economy.

PARADOX

Despite heightened awareness, panoply of new products and services, increasing investment, and concerted efforts from some of the smartest minds in business, government, and academia, the security industry struggles to keep pace.

The number of reported information security incidents around the world rose 48 percent to 42.8 million, the equivalent of 117,339 attacks per day, according to *The Global State of Information Security® Survey 2015* [(1)], published in September 2014 by PwC in conjunction with *CIO* and *CSO* magazines. Detected security incidents have increased 66 percent year-over-year since 2009, the survey data indicates. The same study reports that as security incidents become more frequent, the associated costs of managing and mitigating breaches are also increasing. Globally, the estimated reported average financial loss from cybersecurity incidents was $2.7 million – a 34 percent increase over 2013. Big losses have been more common this year as organizations reporting financial hits in excess of $20 million nearly doubled.

Direct financial costs associated with redressing data breaches and other cybercrime – including forensic investigation, litigation, credit monitoring for identity theft victims, and more – are compounded by the corrosive effect of lost trust. The *2014 Cost of Data Breach Study: United States*[(2)] conducted by the Ponemon Institute found that the average cost for each lost or stolen record containing sensitive and confidential information increased from $188 to $201. The total average cost paid by organizations increased from $5.4 million to $5.9 million. "The primary reason for the increase is the loss of customers following the data breach due to the additional expenses required to preserve the organization's brand and reputation. In fact, the average rate of customer turnover or churn increased by 15 percent since last year," the report concludes.

There clearly are failures in the system. Identifying and rectifying the root causes is essential.

ERRORS OF OMISSION?

Is the failure of the security industry a result of something not being done, or is it doing something wrong?

Lack of investment does not seem to be a factor. Gartner, Inc. reports in its "Forecast: Information Security, Worldwide, 2012-2018, 2Q14 Update" that worldwide spending on information security will reach $71.1 billion in 2014, an increase of 7.9 percent over 2013, with the data loss prevention segment recording the fastest growth at 18.9 percent. Total information security spending will grow a further 8.2 percent in 2015 to reach $76.9 billion[(3)].

Robust spending on information security products and services is eclipsed by R&D investment and an astonishing boom in the birth rate of information security companies. Ellen Messmer, senior editor at *Network World*, wrote earlier this year that "The willingness to invest in new security start-ups is continuing at such a breakneck pace that start-ups still in stealth mode are getting snapped up by more established players before they even publicly introduce their security products and services." [(4)]

So why is the collective security industry – practitioners, consultants, and, yes, technology vendors –unable to curtail, no less repel, cyberattacks? There are multiple contributing factors.

LACK OF SITUATIONAL AWARENESS

Broadly, there is a lack of *situational awareness*. In a 1995 article [(5)] published in *Human Factors: The Journal of the Human Factors and Ergonomics Society,* Dr. Mica Endsley, chief scientist of the U.S. Air Force, provided what is considered the most widely accepted definition of situational awareness. She describes it as "the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."

Applied to the current state of cybersecurity, the methods, meaning and impact of cyberattacks are not assessed in a contemporary framework by those tasked with protecting valuable information assets, personal data, and sensitive infrastructure. Absent a clear read on the cyberthreat landscape, business and the public sector cannot adequately and proactively defend them. Most responses are reactive and in the moment. As a result many are suboptimal and backward-looking.

A gross failure exacerbating the situation is that too many organizations do not objectively assess their security stance. The outcome is a reliance on "status quo" security technologies rather than a threat-focused security program. Acknowledging shortcomings is never easy and sometimes risky and somewhat antithetic to political expediency. However, accepting risk in exchange for a false sense of security is a bad trade.

A lack of situational awareness among many information security professionals is one of the most pressing vulnerabilities in US cyber defenses. One way in which we see this manifest is the false sense of safety some information security professionals feel. There is too much blind faith in the firewalls and other solutions they have deployed. Perhaps motivated by industry hype, a need to check a box on a to-do list, or fear, prudent skepticism and logic are supplanted by urgency for action. Belief is placed in products without true understanding, accurate perception of circumstances, or discrimination. Basic due diligence – evaluations, reference checks, pilot projects – is often overlooked. This fosters complacency and leaves systems exposed. And once solutions are vetted and deployed, vigilance in their upkeeping is imperative.

A FRAGILE FORTRESS

Information security investment on signature- and rule-based prevention technologies such as firewalls and anti-virus software has been disproportionately high compared with spending on solutions that can detect and respond to incursions. Speaking at the 2014 Gartner Security and Risk Management Summit, Neil MacDonald, vice president and distinguished analyst, recommended that "enterprises look to renegotiate the costs of commoditized technologies like anti-malware, IPS and encryption in order to shift that spending to detection and response." [6]

Higher fences and thicker walls appear formidable, but opponents can borrow under, vault over, and even go around them. Some even blend in with the crowd at check points and are allowed to pass. The Great Wall of China is an apt analogy. The iconic structure – built over centuries by successive dynasties –was certainly an engineering feat. But while imposing, the wall was scaled, penetrated, overrun and circumvented many times. Today's "crunchy on the outside/soft on the inside" protection schemes in which a hardened perimeter protects a relatively unprotected and unpatched interior of systems are our modern analogue. After all, defending a 5,000-mile perimeter against determined, fluid enemies who employed swarm tactics was impossible. So it is in the today's cyberwars where there are no real boundaries.

"In the nearly two decades since the first cyber policy discussions were seriously initiated, technology has changed tremendously: Email, the Internet, and mobile devices are now the norm, not unusual like they were in the mid-1990s. The policy debates, sadly, have not changed," wrote Jessica R. Herrera-Flanigan in an article – "Cyber Policy Still Stuck in the '90s" – published on *Nextgov* in October 2014 [7]. Flanigan is a partner at Monument Policy Group, government affairs firm, and a Fellow for Cybersecurity at The National Policy Center, an independent think-tank providing analysis, support and information relating to cybersecurity and innovation issues.

THE SKILLS GAP

Many enterprises lack internal cybersecurity expertise and resources adequate to meet the numerous, well-documented, escalating cybersecurity threats inherent in every aspect of twenty-first century life. This is an unacceptable risk which executive teams and boards of directors have been slow to mitigate, but usually becomes a front-burner priority after a breach has occurred.

EY Center for Board Matters list of six Top Corporate Board Priorities for 2015 [8] included cybersecurity. "Board members were increasingly held accountable, and in some cases ousted, for improperly managing cybersecurity risks in 2014 – risks that will continue to proliferate in 2015," the report notes. Corporate boards must set the tone for enhancing cybersecurity and determine oversight responsibility all the while giving their organizations the appropriate flexibility to embrace the power of technology."

The dearth of cyber security professionals is so acute in the United Kingdom that more than half of 300 senior IT and HR professionals in companies with 500 or more employees told KPMG in a November 2014 survey [9] that they would consider hiring former Black Hat hackers to stay one step ahead of cyber criminals.

The hack of Sony Pictures in November 2014 is a cautionary tale. The network intrusion by unknown parties (later thought to be North Korean agents) resulted in widespread public distribution of confidential information ranging from now infamous emails from the company's former co-Chair mocking President Obama to health records and "dailies" from unreleased films. In an industry notorious for gossip, this was chumming shark-infested waters. Using information from records released by the hackers, *Fusion* reported that of Sony Pictures nearly 7,000 employees, only 11 were on the company's information security team.

Governments, too, have felt the cybersecurity talent pinch. *Government Technology* reported [10] that at a recent Brookings Institution event Michael Daniel, the White House cybersecurity czar, told an executive from the Florida Center for Cybersecurity on the campus of the University of South Florida that the federal government will hire 6,000 computer security experts over the next 18 months.

Why the deficit? A primary reason is that while there are many IT security professionals, cyber security requires different abilities, a distinction that is often overlooked. Cyber security is a subset of information security. However, they are related but distinct disciplines, while both are focused on protecting information systems, the purview of cyber security extends by networks and systems to asset classes such as strategic infrastructure. Power grids and navigation systems are good examples of the latter. Cyber security is also more proactive. There are other qualifications cyber security professionals must possess that are not required of traditional IT. These include an understanding of business processes, the ability to gather, analyze and act on intelligence, and a deep understanding of the entire organization in which they operate."

And there is no substitute for experience. A proper technical and business education is table stakes. It is encouraging to see colleges and universities launch cyber security programs, and federal agencies taking a greater role in funding these programs through efforts like the National Science Foundation Scholarship for Service (SFS) program. The US government recognizes that there is a cybersecurity gap, and that training the next generation of security researchers and practitioners is a top priority. Ensuring the safety and security of governments, industries, and a society at large that is increasingly reliant on cyber infrastructure will take a concerted effort on multiple fronts – not solely in the technical realm. But minting the next generation of cyber warrior takes time and, like any solider, combat is where mettle is tested and skills honed.

In the interim, organizations that lack manpower and expertise can readily avail themselves to a growing number of cloud-based managed security services to augment in-house resources, but often fail to do so. Gartner's MacDonald offers one possible solution, advising that organizations that do not have the in-house staff to support enhanced security response technology should strongly consider one of the growing number of managed threat detection services. [(11)] Organizations considering a Managed Security Services Provider (MSSP) should carefully vet potential candidates just as they should product vendors as all are definitely not created equal. In fact, to properly evaluate an MSSP requires greater due diligence given the increased risk factors associated with outsourcing including key factors like staffing, functionality, and technology infrastructure. Risks associated with outsourcing information security can be even greater since customers are buying a "black box."

NEW, DYNAMIC THREATS; DATED, RIGID APPROACHES

Security practitioners and solutions providers are battling cybercriminals on a greatly expanded threat surface and on an ongoing basis. Advanced Persistent Threats, as the term implies, are complex, constant attempts to breach and bring down systems. A business-driven security approach to security is the only effective strategy for faster, more efficient response, where security teams are certain they are taking the right action.

Understanding the techniques, habits and motivations of threat factors is necessary to stave off an attack when possible or blunt those that cannot be prevented. One truth the security industry has learned is that cybercriminals value the element of surprise. Repelling tenacious, stealthy cyber guerrillas requires a new strategy. The monolithic, static barriers protecting valuable digital assets and critical networks should be augmented with mine fields and trip wires that are difficult for adversaries to identify until it is too late.

Zero-day attacks, named for the time between detection of a new threat and exploitation of vulnerabilities, are a game changer. Think of the adage, "You don't know what you don't know." Preparation for zero-day attacks, by definition, is impossible. Responses must be swift. But this course of action requires an ability to detect and agility to act that many organizations lack.

"With everything happening in business, technology, the threat landscape, there is a spotlight on the information security function right now – it needs to evolve in order for organizations to be successful. As practitioners, we have a unique window of opportunity to really innovate the way we do security," said Roland Cloutier, vice president, chief security officer, Automatic Data Processing, Inc., a member of the Security Business Innovation Council, a group of security executives from Global 1000 enterprises convened by RSA, The Security Division of EMC.

Following are recommendations to can help security practitioners improve strategic planning and tactical responses.

RECOMMENDATIONS

BE PREPARED

The instantly recognizable Scout motto is a brief, yet supremely important truth, which the security industry needs to understand and live by. Today's cyberwars, as this paper has shown, are dynamic. Vigilance and readiness must be inherent in any information security plan. Access control alone is insufficient against foes that attack swiftly and with increasingly frequency using new tools to exploit weaknesses. Adopt and refine an iterative approach to Incident Response. NIST 800-61 or Key Controls defined by the Australian Signals Directorate provide a great foundation to build on. Vulnerability testing and monitoring should be operationalized and ongoing. A holistic response plan incorporating people, process and technology must be established, understood and embraced by all constituents. And the plan itself should be regularly evaluated.

PRIORITIZE

Not all information assets and infrastructure are equal. Decide which are mission-critical and which are business-critical. Identify systems that cannot, for any reason under any circumstance, be breached or taken down. Transaction processing systems and the back-up power grid of a large medical center are examples. Email and business intelligence applications are likely business-critical. Downtime and intrusion would be inconvenient, but tolerable and easier to recover. Understand that cyberattacks are inevitable. Accept that some will succeed. But also know that risk can be managed; loss and damage can be mitigated with advance planning.

ADAPT TO CHANGES IN IT INFRASTRUCTURE

The composition of modern IT infrastructure is increasingly open and amorphous. Cloud computing delivers tremendous business benefits – agility, future proofing, reduced IT infrastructure and support requirements, lower costs. Hosted and managed services are the dominant software models and are here to stay. Similarly, ecommerce, digital supply chains, and mobile networks are indispensable elements of contemporary commerce and communication. Security professionals must understand, embrace and be prepared to defend them with plans and tactics that account for the new, unique security challenges they present.

Eliminate Blind Spots

In the emerging security paradigm, prevention gives way to detection. Granular visibility is paramount to spotting and stopping modern threats. Perimeter security and host AV is not enough. Deploy technology, processes and talent that yield total network and host visibility. Fully-optimize toolsets and orient them to emerging threats, incorporating human intelligence and open source intelligence.

ACCOUNT FOR HUMAN WEAKNESS; ACCOMMODATE THE MODERN WORKFORCE

Humans are imperfect. They are the single softest target for threat actors. Phishing, spyware and other attacks target individuals within an organization. Social media has changed the workplace and opened new entry points for malicious software. Many employees use Facebook, LinkedIn and Twitter to perform their jobs. And even if those and other social channels are not a job requirement, many employers permit staff to take a social media "brain break." An increasingly collaborative workplace means that people are sharing information regularly across offices, time zones and geographies, introducing new sources of risk that must be accounted for.

Just as IT infrastructure has dramatically and irrevocably changed, so has where and how people do their work. Bring your own device reached such a high degree of pervasiveness over the past five years that everyone understands the acronym BYOD. Employee use of personal tablets, smartphones and laptops is no longer the domain of edgy start-ups. Organizations of all sizes and in all industries allow this practice. Many companies encourage BYOD because it reduces CAPEX and improves employee productivity and morale. Couple this with the proliferation of the distributed workforce – employees working from home or a favorite café – and it is easy to see that well-defined, static networks are a relic of a bygone era. Management across the enterprise should develop policies, procedures and a consistent education and training program to ensure everyone in the organization is aware of security protocols and considerations for this new infrastructure.

Trust...But Verify

Abdicating responsibility for critical data and systems is a fatal mistake. Information security providers bring to market more advanced software and services than ever before. Confidence in security technology is well founded. However, insufficient, incorrect or non-existent human-based analysis of security events can render it ineffective. Enterprises must maintain a high state-of-alert and continue to test and strengthen security processes and technology.

CONCLUSION

History provides ample evidence of victors who suffered through early failures and setbacks, only to change tactics and ultimately defeat the most formidable of adversaries. Armed with the knowledge of the root cause of past failures, the way forward becomes clear. These recommendations expose a new approach for organizations to change course and change the outcome from failure to success in the industry's next chapter.

ABOUT RSA

More than 30,000 customers worldwide—including nearly half the global Fortune 500—rely on RSA's business-driven security strategies through threat detection and response, identity and access management, and governance, risk and compliance solutions. Armed with the industry's most powerful tools, enterprises can better focus on growth, innovation and transformation in today's volatile business environment.

Business-driven security enables organizations of all sizes to take command of their evolving security posture in this uncertain, high risk world. Our solutions and services uniquely link business context with security incidents so organizations can reduce risk and be sure they are protecting what matters most.

Appendix

[1] Cybersecurity Incidents More Frequent and Costly, but Budgets Decline says PwC, CIO and CSO Global State of Information Security® Survey 2015

[2] 2014 Cost of Data Breach Study, Ponemon Institute, May 2014 http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

[3] Gartner: http://www.gartner.com/newsroom/id/2828722

[4] Network World: 12 hot security start-ups you need to know, March 18, 2014
http://www.networkworld.com/article/2175279/security/12-hot-security-start-ups-you-need-to-know.html

[5] Toward a Theory of Situation Awareness in Dynamic Systems, Human Factors, 1995
http://uwf.edu/skass/documents/HF.37.1995-Endsley-Theory.pdf

[6, 12] TechTarget SearchSecurity: On prevention vs. detection, Gartner says to rebalance purchasing
http://searchsecurity.techtarget.com/news/2240223269/On-prevention-vs-detection-Gartner-says-to-rebalance-purchasing

[7] "Cyber Policy Still Stuck in the '90s," Nextgov, October 22, 2014
http://www.nextgov.com/cybersecurity/cybersecurity-report/2014/10/cyber-policy-still-stuck-90s/97184/?oref=voicesmodule

[8] "EY Center for Board Matters Highlights Top Priorities for Corporate Boards in 2015," EY company news release, September 12, 2015
http://www.prnewswire.com/news-releases/ey-center-for-board-matters-highlights-top-priorities-for-corporate-boards-in-2015-300018768.html

[9] "Hire a hacker to solve cyber skills crisis' say UK companies," KPMG company news release, November 16, 2014
http://www.kpmg.com/uk/en/issuesandinsights/articlespublications/newsreleases/pages/hire-a-hacker-to-solve-cyber-skills-crisis-say-uk-companies.aspx

[10] "Sony Pictures hack was a long time coming, say former employees," *Fusion*, December 4, 2014 http://fusion.net/story/31469/sony-pictures-hack-was-a-long-time-coming-say-former-employees/

[11] "Florida Colleges Rush to Create Cybersecurity Soldiers," *Government Technology*, January 12, 2015
http://www.govtech.com/education/Colleges-Rush-to-Create-Cybersecurity-Soldiers.html

RSA
www.RSA.com