Navigating A Security Wasteland

Vulnerability Management

Volume 2
January 2018

FIRE AND ICE

Some say the world will in end in fire,
Some say in ice.
From what I’ve tasted of desire
I hold with those who favor fire.
But if it had to perish twice,
I think I know enough of hate
To know that for destruction ice
Is also great
And would suffice.

-Robert Frost

Introduction

Planet Earth. A symbiotic ecosystem nurturing and sustaining life, while facilitating and claiming death. The Internet. A globally interconnected network linking devices worldwide to facilitate communications and improve quality of life, while inviting evil to an infinite environment to commit crimes and exact destruction, including death.

As there are people who still refuse to believe in global warming, there are people who also refuse to believe the destruction our civilization will experience in the wake of a globally impacting cyber event. There are so many parallels we can draw between the earth and the Internet, including the fact that life is unquestionably dependent on both. We have come so far as a species, essentially coming from nothing to the greatest age of invention and accomplishment our kind has ever seen. Why then is it so difficult to believe and take action on the most important matters of our generation? The planet, and life. The answer unfortunately, but most likely, includes an element of politics and greed.

In our first white paper Fighting for Survival in the Age of Cybercrime, we discussed this is some detail. After we released that paper, we realized it wasn't enough for us to call attention to the problem, but that we needed to pull together solutions from experts and share those with our Cybrary community, and hopefully the world. This revelation prompted us to create our newest whitepaper series, Navigating a Security Wasteland. The name may not have directly conveyed the mission we embarked upon, which is why we wanted to share a bit more of our reasoning. We are in fact living in a pre-apocalyptic world of technology. We know the disaster is coming, we just don't know when. We also know the problems we face, we just don't have enough cyber professionals in the world to help us prevent this tragic possibility. Therefore, we at Cybrary will never cease our mission of providing free online cyber training to everyone on planet earth, anywhere, anytime.

Part two of our quest in Navigating a Security Wasteland focuses on technology vulnerabilities, threats, and what we can do to mitigate them in a thoughtful and impactful manner. We turned to Amit Yoran, Chairman and CEO of Tenable to help our readers learn more about the risks and potential solutions to consider. Tenable is a pioneer in the space of vulnerability management, and is innovating new ways to thwart our end in fire. Please read on and enjoy, and look for our final volume in this series coming in March 2018.

Amit Yoran, Chief Executive Officer & Chairman tenable

As Chairman and Chief Executive Officer, Amit Yoran oversees the company's strategic vision as Tenable works to empower organizations to understand and reduce their cyber security risk.

Amit brings to Tenable a unique blend of leadership in the private and public sectors. Previously, he served as president of RSA, leading its transformation into one of the most successful global security companies. Amit joined RSA through the acquisition of NetWitness, the network forensics company he founded and led as CEO.

Previously, Amit served as founding director of the United States Computer Emergency Readiness Team (US-CERT) program in the U.S. Department of Homeland Security. He was also founder and CEO of Riptech, one of the first managed security service providers (MSSP), which was acquired by Symantec in 2002. Amit currently serves as a board member and adviser to several security startups. In addition, he is recognized as a thought leader and influencer in the security industry, and is often sought out to provide expert commentary on his vision for the future of cybersecurity at industry events and in the media.

The vulnerability that attackers exploited to access Equifax's system had a patch available for over two months, why do you think it takes not just Equifax but organizations in general so long to patch vulnerabilities when they know the risks?

For starters, any CEO whose company leverages technology needs to fully understand his organization's cyber exposure and technology risk. Using technology of any kind is not risk free and this requires an increasingly complex cost-benefit analysis in the modern computing environment of IT, cloud, mobile, apps, IoT and DevOps, to say nothing of containers. Foundational security hygiene means that organizations need to know what systems they're running -- there's no other way to truly understand your exposure because you can't protect or maintain what you can't see. Next, organizations need to constantly audit and maintain their systems and this is where so many fall down. Maintaining your systems is not sexy but it gets the job done. And please do NOT rely on a single point of failure here.

How would you define the evolving risk and threat landscape challenge we are facing?

People overestimate zero-day threats. Most sophisticated adversaries use common vulnerabilities and common exploits wherever they can and almost never use a zero-day exploit in isolation. Why? Because they know that most organizations do not act quickly to address a known vulnerability. Why burn a zero-day exploit when you can use a known but unpatched vulnerability to get the job done? I've been asking recently if the whole concept of the advanced persistent threat - or APT - has done more harm than good to our industry. Are we suffering from paralysis and have APTs distracted us from the core issues – the basic and fundamental blocking and tackling – that can make a real difference to our cybersecurity and the safety of our citizens?

> **"...they know that most organizations do not act quickly to address a known vulnerability.**
>
> **Why burn a zero-day exploit when you can use a known but unpathced vulnerability to get the job done?"**
>
> ***- Amit Yoran, Chief Executive Officer & Chairman, Tenable***

In your opinion, how severe is the problem?

The problem is very severe. The status quo is not working. We are in a whole new world of cloud, mobile, SaaS, DevOps, IoT, and operational technology (OT) such as Industrial Control Systems. An asset can be anything from Industrial Control Systems to containers to code itself, making the environment even more complex and harder to secure. This complex mix of digital computing platforms, applications, code and connected devices represents your modern attack surface, where the assets themselves and their associated vulnerabilities are constantly expanding, contracting and evolving - like a living organism. This elastic attack surface has created a massive gap in an organization’s ability to truly understand their cyber exposure at any given time. We call this the Cyber Exposure gap and it represents a fundamental under-representation of cyber risk. The larger the gap, the more significant the likelihood of a business-impacting cyber event occurring.

“If you invest in a technology of any sort, then you should understand both the risks associated with its deployment and the ways in which to maintain and secure it.”

- Amit Yoran, Chief Executive Officer & Chairman, Tenable

How prepared do you think companies are to handle these threats?

Not very -- they can always be more prepared. The vast majority of exploits happened because of poor cyber hygiene and because organizations skip the basic blocking or don’t do it well enough. Despite the proliferation of new tools and technology designed to thwart the latest threat, we still have organizations failing to do the basic level of cyber hygiene needed to stay ahead of cyber criminals. We still have organizations using a patchwork of outdated technology.

How can vulnerability management (VM) help an organization understand their risks and help mitigate them?

Broadly speaking, vulnerability management is about helping organizations identify, prioritize, remediate and reduce cyber risk. The traditional approach is to scan systems and applications for weaknesses at certain intervals -- quarterly or monthly, for example. The problem with this approach is that it’s out of sync with the reality of modern computing. Modern vulnerability management provides continuous visibility into both traditional and dynamic assets -- like cloud and containers -- and delivers clear recommendations on how to prioritize and address vulnerabilities.

How can organizations scan for vulnerabilities on IoT devices?

Most organizations don’t even realize or understand that they have a profusion of devices on their networks. They first need to discover them and they can do that using Nessus network monitor which is designed to discover unmanaged assets among other things.

In your opinion, how often should companies be scanning?

Continuously.

How does “Cyber Exposure” change the way we traditionally think about VM?

Cyber Exposure builds on the roots of vulnerability management but it’s a game changer. Cyber Exposure is an emerging discipline for managing and measuring your modern attack surface to accurately understand and reduce your cyber risk. It transforms security from static and siloed visibility to dynamic and holistic visibility across the entire modern attack surface and in a dynamic computing environment where an asset can range from a laptop to a fighter jet. Cyber Exposure provides live visibility into these assets and will transform security from a raw list of vulnerabilities to a metrics-driven program, where cyber risk is quantified and measured alongside every other organizational risk. This “Cyber Exposure” approach represents a fundamental change in the way that organizations are viewing and responding to their cyber risk.

What additional risks do companies who are using legacy VM solutions and techniques face?

Here’s how many organizations approach cyber today. They’re throwing tons of different security tools at the problem, creating siloed visibility, management overhead and reactive firefighting. They’re relying on a CMDB to get visibility into assets and their configurations, even though 85 percent of these projects fail because of stale data and the fact that CMDBs weren’t built to discover and map today’s modern assets. Or they take a scan-the-network approach to identify vulnerabilities. The problem is that the old one-size-fits-all techniques and tools haven’t adapted for the modern attack surface.

Do you think the government should require and regulate vulnerability scanning?

No, I don’t think the government should require and regulate vulnerability scanning. The government should mandate that organizations understand their cyber exposure -- seems like a fair enough requirement to me. If you invest in a technology of any sort, then you should understand both the risks associated with its deployment and the ways in which to maintain and secure it. A mature vulnerability management program is the best way to do that.

Can you share any predictions you have on the cyber threat landscape?

Until organizations embrace the basic fundamentals of cyber hygiene, we’re going to keep seeing more of the same high-profile breaches we’ve seen over the course of the last year. Just recently, Lloyd’s of London reported that the next big cyber attack could lead to somewhere in the neighborhood of $53 billion in losses, putting cyber crime on par with major natural disasters like superstorm Sandy. We can turn that around and significantly reduce the risk simply by implementing the basics, like knowing and maintaining your systems, so the bad guys can’t use known vulnerabilities to bring your business to its knees.

Kathie Miley, Chief Operating Officer CYBRARY

Kathie has 25 years of experience in the information technology and security field, and is currently serving as the Chief Operating Officer at Cybrary, Inc, the world's first open source platform for cyber security and IT learning.

Kathie has held a variety of leadership roles in the information security and cyber industry including positions at Invincea, RiskAnalytics, Predictive Systems Global Integrity division, NetSec, MCI, Verizon's Enterprise Solutions, CyberTrust and Terremark divisions. Kathie's expertise includes Enterprise Governance Risk and Compliance, Security Policy Assessment and Development, Global Managed Security, Physical Security and Advisory, Cyber Threat and Intelligence, Vulnerability and Patch Management, Identity and Access Management, Security and Network Architecture, and IT Security Training and Enablement. Kathie previously served a board member of the ISSA-DC Chapter, and has held memberships in industry security organizations including ISACA, ISSA, ASIS, HIMSS, and others. Kathie currently maintains her CSX, and carried certificatoions for HIPAA Security Expert (CHSE) and Certified HIPAA Privacy Expert (CHPE).

In your opinion, how has IoT changed the cyber threat landscape?

Last year we witnessed exponentially more technology driven and internet connected devices. Gartner projected 8.4 billion devices connected to the internet in 2017– growing to 21 billion by 2020. This attack surface is unimaginably large, and is essentially a playground for cyber criminals. Hackers will exploit new and unknown vulnerabilities, and even discover old vulnerabilities still hidden in IoT devices. There is no doubt their successful exploitations will result in catastrophe – including the death of innocent people. Our quality of life today has become absolutely dependent on the resilience of IoT, versus IoT being a simple convenience. We continue to find old web vulnerabilities on home IoT devices, medical devices, and many others. Humans simply cannot keep up with the expanding scope of the problem, which makes it impossible to identify, monitor, and manage the entire breadth of these devices.

IoT manufacturers must build security into their devices at inception. Especially when those devices sustain life as we know it.

How do you think that companies should be training their workforce on vulnerability management?

Training in vulnerability management is not just a cyber security team responsibility, it is a human responsibility. Companies must embed cyber responsibility into the DNA of their organizations, and stop assuming that users are too ignorant or too lazy to handle it. Eventually in human history, individuals took responsibility for the protection and safety of our communities, property, and families. We simply had no other choice. There isn't any one patrolling the grounds of my home to ensure I lock my doors, turn off the gas on the stove, or defend my home from intrusions. There was no home and life safety course available in school. The only thing I knew for certain was that I needed insurance for my property in response to a disaster. I had to learn to manage how to prevent disaster and protect everything for the sake of my family's welfare. The point being that people can learn and want to learn when they understand the importance. It is incumbent upon us in the cyber field, and at the highest levels in corporate or government agencies, to continuously train staff at all levels to understand the risks and the consequences of poor security hygiene. Let them learn and become part of the solution.

"Training in vulnerability management is not just a cyber security team responsibility, it is a human responsibility."

-Kathie Miley, Chief Operating Officer, Cybrary

Specifically, training programs within organizations should be distinct to their role, identify critical assets, and expose employees to the impact of vulnerabilities to the organization, their job, and their customers or stakeholders – especially when their work touches an aspect of physical human safety.

When it comes to vulnerability management, how do you prioritize risk?

Risk is defined as the exposure of potential loss or damage. As it pertains to cyber, traditionally, we look at availability, integrity, and confidentiality of information technology systems and data. Risk prioritization has to center on the potential impact to the company, agency, or specific mission, were it to experience an impact of key capabilities, financial loss, reputational damage, or given the rapidly emerging IoT landscape - loss of life – were a cyber event to occur. To prioritize risk, it is mandatory that every organization continually assess vulnerabilities and address them as quickly as possible, focusing on the severity of the supported business function and potential impact.

"There is no doubt their successful exploitations will result in catastrophe – including the death of innocent people."

-Kathie Miley, Chief Operating Officer, Cybrary

How do you create the right reviews/reports for the right stakeholders in terms of vulnerability management?

There are many opinions on how to report on vulnerabilities, the frequency of such reports, and to whom they are shared. My opinion is leadership in all departments need to be made aware of the vulnerabilities of their specific IT assets so they can participate in solving the problem as a priority vs. never knowing the problem existed. Commonly, IT will do an assessment, find the vulnerabilities, and then create a patch and/or risk mitigation plan. In my experience in running businesses – I was never approached by IT and offered to review the risk exposure my team had created by installing something, or connecting to a third party. IT handled it or perhaps didn't get around to handling it and did not always have a good connection to business risk and business impact. In fact, no IT team has the capacity to patch every vulnerability and mitigate every risk. I don't think there is a need to report to everyone, as that would be advertising the risk exposure to broadly. But, at a minimum, vulnerabilities should be shared across key business units, including their priority and the overall status of a vulnerability management program should be provided to senior leadership and the board.

What Is the Risk Exposure for Executives and Officers from Cyber Events?

I am a broken record on this topic. I adamantly believe that unless C-Level executives and boards have cyber security as a top risk management agenda item, we will continue to see more and more successful attacks, collapse of communities, countries, and loss of life. The leaders set the tone, the level of risk tolerance, but also the amount of management support for the program and allocation of resources and budget. They cannot do that effectively if they are not aware of the cyber risks their organizations face every minute of the day. If not well prepared, it could affect their jobs, and overall company sustainability.

What is your advice to organizations for staying current on cyber trends, news, federal, state, industry and international data security regulations?

Continuous learning should become a non-negotiable requirement in every organization, at every level. This requirement also includes participation in industry associations working in their field and vertical market (e.g., oil and gas, or financial services) to understand key industry issues. Further, key individuals must stay abreast of applicable compliance requirements (e.g. GDPR), and have an action plan in place. In a recent survey by Cybrary, we found that over 90% of respondents said their employers do not pay for any cyber training or certifications, let alone continuous learning. This has to change. If money is the issue, look no further than Cybrary. We offer unlimited free video-based cyber training for individuals, companies, governments, education, non-profits, and many others. We enhance that training with custom curriculums, practical hands-on labs, mock scenarios, practice exams, micro-certifications, and much more, for less than the cost of one week of training in a traditional brick and mortar facility.

How do organizations address the cyber skills gap in the face of so many new vulnerabilities?

To say that training and certifications is the answer, is incorrect. It is “an” answer. However, the biggest challenge we face is finding the people who possess the requisite skill sets, or the desire to learn. There is no place on earth where cyber learners and companies can come together under a common cause, which is to fill the 2 million open cyber jobs. Cybrary brings these two massive communities together. Not unlike a dating service, learners will be able to search for their ideal position and employer, and employers will be able to search for their ideal candidates, in a dedicated cyber-only community. Not only that, but employers will have full transparency to what the actual technical proficiency is of each learner, via the rapidly expanding catalog of assessments. Today that is our best approach and what Cybrary will deliver to the market in early 2018.

> **“It is incumbent upon us in the cyber field, and at the highest levels in corporate or government agencies, to continuously train staff at all levels to understand the risks and the consequences of poor security hygiene.”**
>
> ***- Kathie Miley, Chief Operating Officer, Cybrary***

Tenable™, Inc. is the Cyber Exposure company. Over 23,000 organizations of all sizes around the globe rely on Tenable to manage and measure their modern attack surface to accurately understand and reduce cyber risk. As the creator of Nessus®, Tenable built its platform from the ground up to deeply understand assets, networks and vulnerabilities, extending this knowledge and expertise into Tenable.io™ to deliver the world's first platform to provide live visibility into any asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, large government agencies and mid-sized organizations across the private and public sectors.

Contact:

Tenable
sales@tenable.com
www.tenable.com
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

Cybrary is an open-source cyber security and IT learning and certification preparation platform. Its ecosystem of people, companies, content, and technologies converge to create an ever-growing catalog of online courses and experiential tools that provide cyber security and IT learning opportunities to anyone, anywhere, anytime. Cybrary levels the playing fiel for those who want to advance in or start a cyber security or IT career by providing anyone with accessto the tools they need to be competent and confident.

Contact:

Cybrary, Inc.
bizdev@cybrary.it
www.cybrary.it
7833 Walker Drive
Suite 510
Greenbelt, MD 20770