



Navigating a Security Wasteland

Endpoint Protection & Prevention

Volume 1
December 2017



CYLANCE™

Preview of Cybrary's *De-Classified Report* : Coming January 2018



1,2,3, 2017 Cybrary Community Survey

Introduction

Not very long ago, the notion of automatically preventing security incidents was considered too risky. The concern was that a legitimate process would be blocked that could negatively impact the business, or cause an executive a bad experience. Both scenarios would be blamed on the security team, which would threaten their personal job security. In the end, the user experience was put ahead of risk reduction. There is not necessarily anything wrong with putting user experience first, especially since in the early days of prevention solutions, the technology was not mature and unable to deliver seamless security.

Today technologies exist that are virtually invisible to the end user, and since they operate on various forms of machine learning / AI, are able to reduce risk of malware related incidents down to almost zero. Layer onto these endpoint security solutions strong identity management and encryption, and you have a fantastic proactive, prevention, and data protection system in place. The industry is filled with many different endpoint security solutions, making it difficult for security professionals to determine which solution is the best for their environment. At Cybrary, we partner with some of the world's leading endpoint detection and prevention solutions, making our members aware of them and providing necessary training to fully understand the technical depth of each solution.

Choosing a technology is a major challenge, but technical superiority is not the only criteria one should be considering. You could have the best solution in the world, but also have an uncertain mission and vision of the company. Perhaps you select a solution that is amazing, and has an amazing company behind it – but it doesn't work on all of your technology platforms. Maybe it does not offer support on Macs, or on Linux Servers, or older versions of Windows that you still have in production. Whatever it may be, there will never be a perfect solution, right?

In our research on companies offering endpoint security, we found Cylance to be a well-rounded, well-managed company, with a solid vision and customer first culture. We are therefore excited to have sat down with one of the world's top security professionals, Malcolm Harkins who is the Chief Security and Trust Officer at Cylance. Malcolm shared with us his thoughts and advice on endpoints so we could share that knowledge with our Cybrary members. This is the first in three whitepapers written specifically for our members on industry thought leadership and innovation. We conclude with the importance of continuous learning as it pertains to the topic in the whitepaper. We hope you enjoy the paper, and reach out to us with your thoughts.



Malcolm Harkins, Chief Security & Trust Officer



Malcolm Harkins is the Chief Security and Trust Officer at Cylance Inc. In this role he reports to the CEO and is responsible for enabling business growth through trusted infrastructure, systems, and business processes. He has direct organizational responsibility for information technology, information risk and security, as well as security and privacy policy. Malcolm is also responsible for peer outreach activities to drive improvement across the world in the understanding of cyber risks as well as best practices to manage and mitigate those risks.

Previously Malcolm was Vice President and Chief Security and Privacy Officer (CSPO) at Intel Corporation. In that role Malcolm was responsible for managing the risk, controls, privacy, security, and other related compliance activities for all of Intel's information assets, products, and services.

Before becoming Intel's first CSPO he was the Chief Information Security Officer (CISO) reporting into the Chief Information Officer. Malcolm also held roles in Finance, Procurement, and various business operations. He has managed IT benchmarking and Sarbanes-Oxley compliance initiatives. Harkins acted as the profit and loss manager for the Flash Product Group at Intel; was the general manager of Enterprise Capabilities, responsible for the delivery and support of Intel's Finance and HR systems; and worked in an Intel business venture focusing on e-commerce hosting.





“Organizations are suffering from alert fatigue and detection deficit disorder. They are playing whack-a-mole constantly and they struggle to keep up.”

-Malcolm Harkins, Chief Security & Trust Officer, Cylance Inc.

Malcolm previously taught at the CIO institute at the UCLA Anderson School of Management and was an adjunct faculty member at Susquehanna University in 2009. In 2010, he received the RSA Conference Excellence in the Field of Security Practices Award. He was recognized by Computerworld as one of the Premier 100 Information Technology Leaders for 2012. (ISC)2 recognized Malcolm in 2012 with the Information Security Leadership Award. In September 2013, Malcolm was recognized as one of the Top 10 Breakaway Leaders at the Global CISO Executive Summit. In November 2015, he received the Security Advisor Alliance Excellence in Innovation Award.

He is a Fellow with the Institute for Critical Infrastructure Technology, a non-partisan think-tank providing on cybersecurity to the House, Senate, and a variety of federal agencies. Malcolm is a sought-after speaker for industry events. He has authored many white papers and in December 2012 published his first book, *Managing Risk and Information Security: Protect to Enable®*. He also was a contributing author to *Introduction to IT Privacy*, published in 2014 by the International Association of Privacy Professionals. The 2nd edition of Malcolm's book, *Managing Risk and Information Security: Protect to Enable®*, was recently published in August of 2016. Malcolm has also testified before the United States Senate Committee on Commerce, Science, and Transportation on the "Promises and Perils of Emerging Technology for Cybersecurity."

Malcolm received his Bachelor's degree in Economics from the University of California at Irvine and an MBA in finance and accounting from the University of California at Davis.



“Leaders also need to take risks by running to the risky things in order to shape the path of risk proactively vs. try to stop the innovation cycle and slow the organization.”

-Malcolm Harkins, Chief Security & Trust Officer, Cylance Inc.

What are a few lessons you think everyone can learn from the Equifax Breach?

1. Don't believe the hype of it's the "worst breach ever for consumers." It could be impactful to some consumers but with all the other data breaches that have occurred the past several years the chances are a lot of the same data was already exposed in some cases, more sensitive data was if you had health records breached or received a notification from the OPM breach.
2. Not everything will ever get patched or be patched. Mistakes can occur, changes can occur, and we must also remember that patches also generate risk. Why? Because a patch is a change and change introduces risk which is why it is not as simple as some people will think. A patch can create operational downtime or break other applications from working or introduce a new potential vulnerability.
3. Integrity and intent matter.

What would you say are the most prominent threat actors we are dealing with today?

There are variety of threat actors and threat agents that are trending up in their activity. But I think this is the wrong question and one we spend too much time as an industry focused on. As a CISO/CSO I have no ability to control the threat actor (although there are insider risk triggers that an organization can reduce or increase). The motivations across the actors may differ but the tools, tradecraft, methods are very very, similar.

Malware is top of mind for most organizations, what steps can security teams take to prevent infection?

1. Starting with the basics – good IT architecture, hygiene, configuration management.
2. Get rid of the legacy solutions that not only don't stop the malicious code but also degrade the user/computing experience.
3. Deploy a solution on your systems that is a lightweight agent that doesn't require constant updating. The ideal solution should have the same efficacy to prevent malicious code when connected to the network or when the system is offline. The ideal solution needs to be a single agent that should also offer enhanced features to deal with memory exploitation, script control, device control, and application white listing.
4. Stop blaming the user – if bad things happen when a user opens an attachment or clicks on a link – that's a technology failure.
5. Demand the creators of technology to do a better job of security development life cycle to reduce vulnerabilities prior to its release.

When it comes to prevention methods and identifying risk, in what ways do you see your customers struggling to keep up?

1. Organizations are suffering from alert fatigue, and detection deficit disorder. They are playing whack-a-mole constantly and they struggle to keep up. This is where organizations need to rethink the traditional approach and find solutions that will allow them to do 3 things: 1) Create a demonstrable and sustainable bend in the curve of risk 2) Lower or flatten total cost of controls 3) Reduce the control friction that security has on the business, the user, computing.
2. Organizations are adding more technology, software, apps constantly as well as 3rd parties – have efficient processes to handle these so they can be dispositioned for risks and determine what controls may be needed is also key.
3. Justifying budget and existence.

A lot of companies are turning to third parties for various security-related services, what do you feel are the risks associated with relying on third parties?

Depending on the organization and their internal competencies this can greatly reduce risks. But one needs to remember you cannot outsource your responsibility/accountability for managing the risks. You can outsource tasks to help you manage things to third parties but at the end of the day if you have an issue you're still accountable regardless of who is doing the work.

For organizations who outsource security services, how is assessing third-party risk in those situations different from assessing your own?

Well, the perspectives are different – an employee vs. a contractor. Who has a stronger sense of ownership? It boils down to competencies, cost, and culture. Whether you in-source it or outsource you need to look at those three things.

Do you think lack of knowledge and the overwhelming number of vendors in the space play a role in the decision making when it comes to what solutions a company implements into their strategy?

Yes. And the marketing machinery of the industry adds to the confusion not only for CISOs, but for the analysts who cover it and also profit from the very vendors they are evaluating. So, think about the motivations of all the players, how they make their money, and judge if they are incentivized truly for your best interest.

How can a security professional who is still learning break through the noise of the crowded market and learn how to properly identify what solutions are right for their organization?

Talk to other peers, do real testing for yourself, never pay for a pilot or proof of concept.

What can leadership do to help keep their teams informed and minimize their overall risk as an organization?

Leadership is the art of motivating others to struggle for shared aspiration. So, leadership needs to continue to communicate, motivate, and inspire. Leaders also need to take risks by running to the risky things in order to shape the path of risk proactively vs. try to stop the innovation cycle and slow the organization, which results in the business going around the security team - resulting in more risk and more cost to the business.

How do you think Artificial Intelligence (AI) is changing the way we think about our security and threat prevention strategies?

Artificial Intelligence is progressing rapidly with everything from SIRI to self-driving cars relying on it automate specific tasks. AI is revolutionizing what is possible so we can not only re-invent but re-imagine how to do security as well. AI as the core of a new security architecture has already shown that it can do a significantly better job at preventing the risks at the core of the cyber risk cycle – malicious code.

A control architecture should assume that attempts at compromise are inevitable—but we should also understand that it is possible to achieve real prevention for 99% or more of risks that could occur, including that of malicious code and zero-day attacks caused by mutated malware. Should a piece of malicious code attempt to execute, we can instantly apply artificial intelligence and machine learning to analyze the features of files, executables, and binaries in milliseconds to stop the bad code dead in its tracks before it has a chance to harm the environment. With this approach you can move from a state of reaction/response where your risks are higher, your costs are higher, and your security team is fatigued by alerts and incidents to one where they can more effectively and efficiently manage the risks.

In the future, artificial intelligence and machine learning will also be able to solve other vexing security issues that we face today such as passwords and identity management used to authenticate and authorize users. We will also be able to mitigate distributed denial of service attacks using the ability to predict and thus prevent in automated fashion the flood of requests that can so easily disrupt an organization today.

Join Cybrary's Kathie Miley & Cylance's Malcolm Harkins for an in depth webinar discussing "Navigating a Security Wasteland" on December 13th, 2017 at 3:00 PM EST

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, Certified HIPAA Security Expert (CHSE) and Certified HIPAA Privacy Expert (CHPE).

How can security professionals learn about what solutions are out there and which ones are right for their business?


There are many resources available to find information on vulnerability management and endpoint solutions. Gartner, Forrester, IDC, and Frost and Sullivan are a few of the professional analyst firms who review products and make available the results of their findings in the form of stack rankings and pro vs. cons summaries. Cybrary hosts a great deal of training on various products in each of the categories covered in this report. A member or business can search by the topic or vendor name to get a better understanding of some solutions and functionality. Being able to take the training courses – for free of course – also gives some insight into the usability and efficacy early in the evaluation cycle. Specifically, in partnership with Tenable, Cybrary hosts a great deal of training as well as access to Tenable webinars and other content.

Does someone have to be certified to have the jobs necessary to manage vulnerability scanning and malware prevention solutions?

Certification requirements depend on the needs of the employer, which can wildly vary. Although in many cases, certifications are not required, they are a fantastic way of demonstrating to your prospective or current employer, that you have the qualifications necessary to perform the duties aligned with a given subject or product vendor. For example, carrying a CISSP lets the world know that you have knowledge, experience, and credibility in the information security profession. Given the shortfall in IT and Cyber Security professionals in the world today, technical and specific practitioner certifications could even be weighted with more value than a degree. In my organization, were I interviewing a candidate who had a degree in Zoology and a candidate who had a CISSP, I would put more weight on the CISSP. But then again, I don't manage a Zoo.

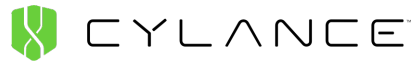
Are companies facing retention issues with employees who are managing these types of solutions?

Yes, undoubtedly. Some of the technology that vendors are using today were not in practical existence a few years ago. I graduated in the 1980's, and other than in the "The Terminator" – there was no real mainstream use of Artificial Intelligence in technology when I went to school. Learning these new innovative applications requires that one seek training and certifications on a continuous basis. There is no final stop for gaining knowledge. It is something everyone does every day and something we all must do to keep our skills and expertise relevant. Had I ended my learning at school – I would have never entered the technology field. I would be a starving artist surviving only on my pencils and paper (and often my eraser).



“Learning these new innovative applications requires that one seek training and certifications on a continuous basis. There is no final stop for gaining knowledge.”

-Kathie Miley, Chief Operating Officer, Cybrary Inc.



Cylance® is revolutionizing cybersecurity with products and services that proactively prevent, rather than reactively detect the execution of advanced persistent threats and malware. Our technology is deployed on over ten million endpoints and protects hundreds of enterprise clients worldwide including Fortune 100 organizations and government institutions.

Contact:

Cylance
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue
Suite 700
Irvine, CA 92612



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 field for those who want to advance in or start a cyber security or IT career by providing anyone with access to 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