SNS SUBSCRIBER EDITION • VOLUME 22, ISSUE 32 • WEEK OF SEPTEMBER 4, 2017

THE STRATEGIC NEWS SERVICE©

GLOBAL REPORT ON TECHNOLOGY AND THE ECONOMY™

SPECIAL LETTER

CYBER SECURITY IS EVERYONE'S BUSINESS

by Ray Rothrock

SNS: Special Letter
Cyber Security Is Everyone's Business

By Ray A. Rothrock

FiRe 2017™

"Breaking Through"

The 15th annual
Future in Review conference

In This Issue
Week of 9/4/2017 Vol. 22 Issue 32

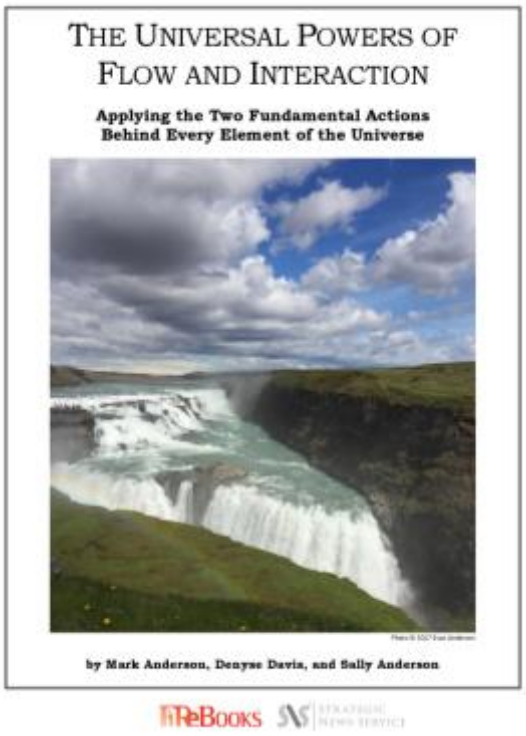
FEATURE:

Returning to the beautiful
Stein Eriksen Lodge Deer Valley
Park City, Utah

www.futureinreview.com/register

Recommended Reading

The First Book on the World's First Principles, published this week in its first edition:



"You have achieved what Leonardo aspired to." – Curtis Wong, Principal Researcher, Microsoft Redmond Research Lab; and Trusted Expert, Bill Gates' Codex Leicester

TO GET YOUR COPY NOW, JUST CLICK HERE FOR A SPECIAL, ONE-WEEK PRICING OFFER FOR SNS MEMBERS ONLY:

https://store.stratnews.com/shop/universal-powers-flow-interaction/

***Publisher's Note*:** In security circles, it has long been a poorly kept secret that the tools of the time – firewalls, antivirus, and malware protection – were what scientists would call "necessary, but not sufficient" to the task of protecting the vital secrets of our companies and countries.

In fact, it was much worse than that.

I once was in a conversation with the top security official in the UK, who was (properly and proudly) discussing how working with the private sector was going to

eliminate 90% of cyber attacks. "That's great," I said. "But who cares, when they'll still be vulnerable to 100% of the state-sponsored attacks on their crown jewels?"

Even today, as this week's well-qualified author points out, anyone assuming that their tools and spending on security can keep the bad guys out of their networks is just dreaming. A determined state-sponsored team from a growing list of countries who make it their business to steal and then dominate yours will get through.

Who are these teams? In order of number, China represents about 95% of all cyber-based IP theft. In terms of order of activity, a rough approximation would put China first, followed by Russia (better, but more interested in military and policy), and then the flotilla of Iran, DPRK, perhaps even Pakistan, and others coming closer every month. It doesn't take a large population, or a large military, to create a large cyber-threat presence. The obverse of this is also true: the US is the most vulnerable nation in the world with regard to cyber attack, because we have the largest dependency on computers and the net. We are also *not* the most advanced attack team, by private estimates, with even DPRK ahead of us in offensive weaponry.

All of our members will want to catch up on the latest in protecting their corporate secrets. Read on. – *mra*.

SPECIAL LETTER:

CYBER SECURITY IS EVERYONE'S BUSINESS

By Ray A. Rothrock

Deception Is Nothing New

Long before there was a "cyber," people were skilled in the practice of misinformation, stealing information to sell, encryption to protect information, and all the tools of the spy trade now made easier by the internet. My favorite use of misinformation was by Benjamin Franklin during the War for Independence in 1776, in order to gain advantages with foreign governments. And of course, depending on your age and interests, Operation Fortitude, conducted by General Patton's Ghost Army, was possibly the greatest deception in modern warfare (except maybe for the Election of 2016), leading to a successful invasion of Europe

in World War II. But regardless of your politics or recollection of history, deception and tricks are as old as civilization itself.

Today, however, deception by cyber has come into a new focus, to a new height in our awareness. It's personal. And it's become pervasive. The headlines are full of stories about cyber attacks against corporations and governments. Most people don't know whether it affects them or not, but we all know someone who's had their identity stolen. And all of our information, even critical credentials, is probably out there on the dark web for sale and pilfering.

Cyber threat is now front and center. It touches each and every one of us. And it exposes us all to the seedy side of our digital lives. There are no secrets. Scott McNealy of Sun Microsystems was right when he said: "Privacy. Get over it." He wasn't exactly prescient with the comment – just a few years ahead of when any of us would understand it.

Importantly, because of the state of our networks, our policies, our spend, and our history, every corporation is at risk of a cyber attack or other cyber event. As I'll explain in this letter, the attackers and their malware are already in your network. You can't prevent them from making their way in, and you may not be able to detect it, or even know it's happening. But it is, and they're lurking and hunting for their target.

Today's security products are essential to controlling and gaining an understanding of your readiness. But they are not sufficient as a manager of your company. What is in your control is what you are able to do when they reveal themselves. That requires knowledge, readiness, and resilience.

In the Beginning (It Was Fun)

The digitization of our lives began with the advent of the internet and the World Wide Web in the early 1990s. In the beginning, it was fun. Browsing on a Mosaic browser in 1993 to cool science sites at national labs, or even cutting-edge companies, was very exciting. As quickly as the technology spread, the ideas of how to use it spread, too. Not only was the WWW good for finding information about places, people, and things, but suddenly you could buy something remotely. I'll never forget when my partner at Venrock, Dave Hathaway, asked me to demonstrate an actual credit-card transaction on the web. In 1994, that was not easy to do, for the lack of commerce sites, unless you found a porn site. Yep – porn led the way for commerce.

But this digitization really is about economics. It always has been, whether it was counting votes on an IBM card-reader machine or cloud computing. It's about shortening the time it takes to get things done, removing friction in a transaction, and turning physical into digital – as fast and as cheaply as possible.

Gone are the days of ruled paper and accountants in green eye-shades writing transactions in books. Those ink-and-paper transactions quickly went by the wayside when accounting ledgers were put on mainframes. Amazing, the transformation and the speed of it.

Those systems were largely self-contained units of computing, operated by specialists in glass air-conditioned rooms. To touch a computer was impossible. Many us remember handing punch cards with the code for our programs to an operator who would feed the machine and give us back a printout in the morning. We didn't even know where the computer was. Then along came CRT terminals, like the VT-100. No punch cards required. Just write the code on the screen, save it in a file, and say RUN. Instantly, the answers – or the errors – came back in your face.

My first glimpse into the odd world of cyber was through the book *The Cuckoo's Egg*, by Cliff Stoll. It's a remarkable Cold War–time story of cyber espionage through mainframes, uncovered by an under-employed physicist at a national lab who found a few penny errors in billing that led him to a back door in the lab's mainframe which was operated by the East Germans.

I was a young practicing engineer when the Apple II and the PC were thrust into the world. These were incredible standalone computers of which you literally had full control. Shortly thereafter, Sun Microsystems began shipping machines with networking built-in. The not-quite-standard TCP/IP protocol suddenly became the standard. When Tim Berners-Lee came up with HTML and the WWW – well, the horse was out of the barn. We have all lived this history over the last three decades or so. And how awe-inspiring it is.

What most of us don't know is how it has all been built, and built cheaply. How it wasn't really designed for security. We know, of course, the ARPA-NET was supposed to survive nuclear attacks, so by design it was open and was always a best-efforts architecture. Nowadays, that's how *not* to build a secure network. Along the way, many more-powerful and -secure networking protocols were introduced by the likes of IBM and others. But while very secure, they were not cheap. And when people wanted to connect to "cheap" TCP/IP networks, it was hard and expensive. Eventually, everyone just gave up and went with TCP/IP. Today we're seeing amazing distribution of TCP/IP-connected things in what is called the IoT – the Internet of Things.

Early Malware

I love the word "malware." "*Xxx*ware" is like "*xxx*gate" – à la Watergate. We have morphed more words into "*xxx*ware" in the computer business. Even the core components – software, hardware. But malware – that is the bad stuff. A very apt word. Some of the earliest malwares were simple things that high-school geniuses

wanted to try out. Distribution was hard, so somehow they got it on floppy disks, and all those Apples and IBMs used floppy disks. Computers were not networked in the earliest of days, so it was a physical transfer from floppy to computer, then computer to floppy, and on and on.

Then networks started putting computers together. Really only local area networks, or LANs. But then the commercial internet happened. With the advent of the ARPA-NET for defense, the commercialization of this seminal technology of TCP/IP, and Ethernet, everyone wanted to be connected. I recall at Sun Microsystems my introduction to Metcalfe's law, about the power of a network being proportional to the N^2 of the endpoints. We all knew Moore's law was powerful (it is, make no mistake), but Metcalfe's was mind-boggling in terms of the impact of being able to get information and talk to other people through a computer.

Those connections have driven the business world to digitization of more and more of their business. Business is online. Digitized business is cheaper. And businesses are all about profits. Over 50% of businesses address their customers through the web. The transformation from face-to-face business to web-based business is remarkable, powerful, and unstoppable. As technology has enabled more and more capability, commerce has taken advantage of that. I can only imagine the impact that artificial intelligence and similar technologies will have on our ability to interface with a computer and accomplish what's needed to do business.

Those connections empowered many people with information and learnings – all of this shrinking the world as we know it. Email is a good proxy of just how powerful that endpoint connectivity is. Today, about three billion people in the world have email accounts, to say nothing of all the other accounts across Facebook, Snap, Twitter, and the like. Social media is the network, plain and simple.

Here are some stats that will blow your mind:

Every minute:

- Facebook users share nearly 2.5 million pieces of content.
- Twitter users tweet nearly 300,000 times.
- Instagram users post nearly 220,000 new photos.
- YouTube users upload 72 hours of new video content.
- Apple users download nearly 50,000 apps.
- Email users send over 200 million messages.

And today, we have to consider things like toasters, cars, fitness watches, and other devices that are connected to the internet. The IoT has exponentially accelerated the attack surface, as it has become known.

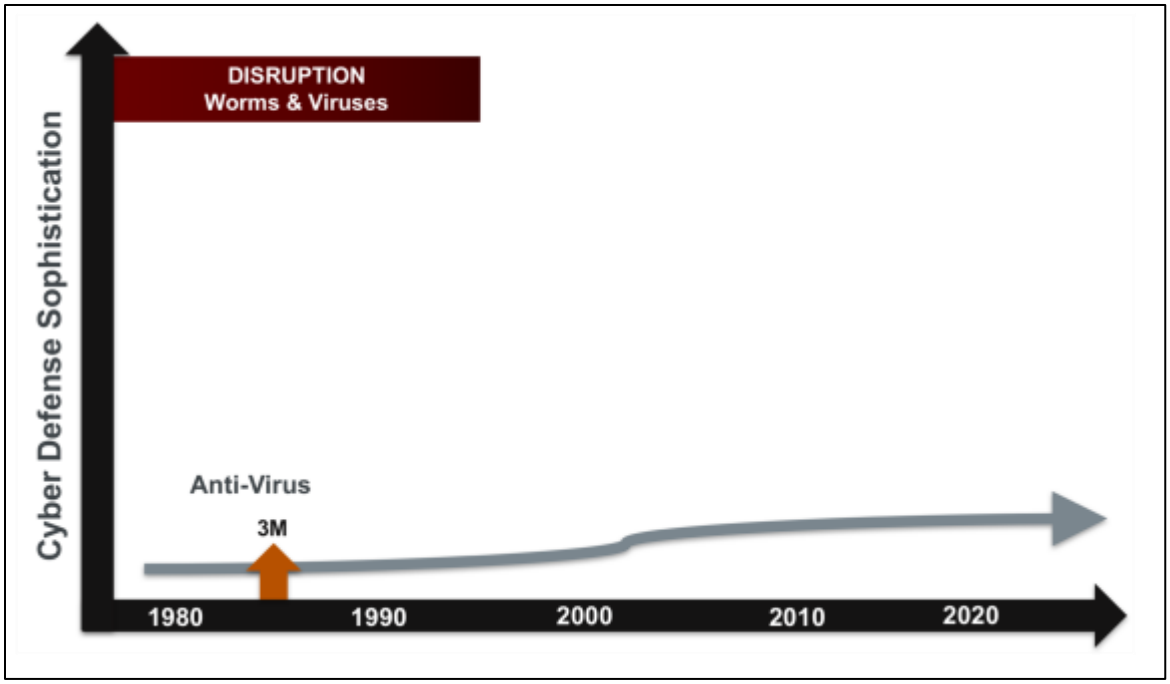
My venture career at Venrock covers this transformation – from a mainframe world to a social-media-networked world – and all the phases in between. Early on, it was clear that while the internet would create tremendous excitement and wealth, there were risks involved, and those risks we probably still don't appreciate or even completely comprehend today. In fact, I would venture to say that the business world is only now, in the last handful of years, coming to grips with the impact of cyber security and what it means for their business. Nothing is learned instantly, but today *cyber is everyone's business*.

The Evolution of Cyber Security

In the last 30 years, the strategy for people who implement cyber-security solutions against threats has been pretty much the same: identify a problem and create a point solution. Or identify a threat and create a point solution. In the early days, it was about one computer, not a group of computers on a LAN. The issues were rarely taken to the boss, as the software – antivirus programs and such – was cheap, easily implemented by those who owned a desktop computer, and required very little management.

The real purpose was *disruption*, sometimes just to see if it could be done, by a "criminal," likely a 15-year-old kid. Usually the attack was only one-way – get the malware in, and see if it causes problems – because networks barely existed, and talking to the malware from the outside hadn't been invented yet. In the earliest of days, two major enterprises were built to solve this very basic problem of virus disruptions. Those companies were Symantec and McAfee. With each new threat, new solutions were invented – or, in the case of a new virus, a new signature was recognized that could be distributed to prevent computers from getting infected. This method of dealing with viruses stands today, and is a pillar of cyber security worldwide.

The chart below, which I will develop over the course of this letter, illustrates the continuity of antivirus solutions over time. While the numbers varied in the early days of antivirus, today there might be upwards of 3 million attacks that the AV solutions address.



Cyber Crime and Network Security

People like real, physical-world analogies in order to understand things. Digital networks and cyber are no different. As companies connected their LANs to other company LANs via WANs and the internet, the notion of a doorway, or gateway, evolved. The term for controlling that access at the WAN access point is *firewall*. Firewalls are not new in IT. But they were new in the internet world. Firewalls, like the term suggests, keep the bad things (fire) on the outside. This is akin to a front door on your business that requires a key card to identify you, or simply a key to unlock. In time, it was suddenly easy to penetrate a company's network from afar. This was the beginning of a very new threat that the commercial world really had not thought much about. Since the digital front door was mostly open, the bad guys – not just mischievous high-school kids anymore – digitally walked in, and early cyber crime started.

Like most technology markets, there was a tornado market in the mid- to late 1990s, with dozens of companies vying for dominance, as thousands of corporations quickly implemented firewalls to *prevent* the bad guys from getting in. Only a few survived – namely Check Point Software, Palo Alto Networks, and Fortinet. While each of these vendors has a multitude of technologies built into their gateways, the bottom line is that they are gateways, or firewalls. (This is a typical technology cycle.)

This worked for a while. However, as good as firewalls were, they weren't capable of keeping everything out. So people thought we needed technology to detect

anomalies on the network. Thus, intrusion detection and intrusion prevention were invented. That is: assume something got inside – how would you detect or see it? Again, a wave of companies emerged, with few surviving. Now IDT – or IPT, as it is known – is often built into the firewall or other routing equipment, since every packet can be inspected as it flows in, out, and around. (Moore's law greatly made CPUs powerful enough to do this in real time.)

Now that it was easy to distribute malware through the front digital doors, it could be programmed to do lots of things – like keystroke loggers, or impersonators, or just listeners – making it easy to spy on another's network. It could even be manipulated from the outside – command and control, as it's known – once it found its target.

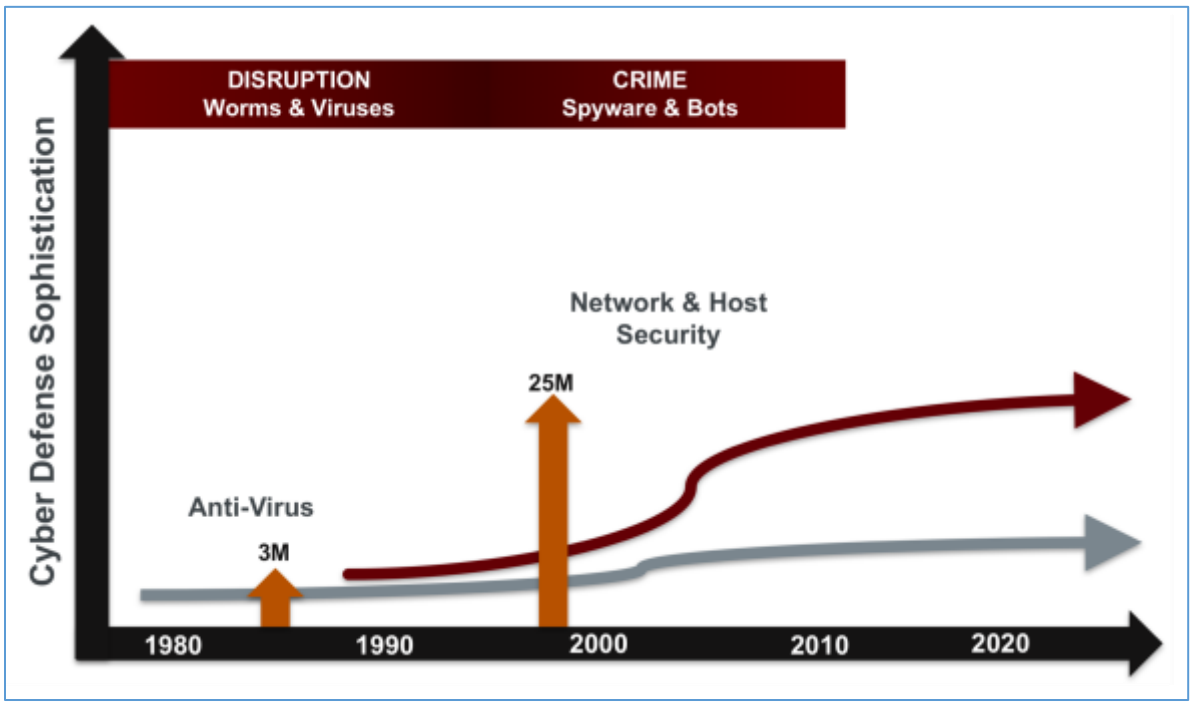
As firewalls became more capable and intrusion systems were deployed, this meant that someone now needed to manage the network. These systems were sophisticated, and as they became a corporate resource, the money spent to build and manage them started to show up in the budgets of IT departments. The cyber industry grew from a $99 antivirus solution – often purchased by a single individual to protect a single computer – to a $10,000 firewall and intrusion detection system to protect a full network, requiring constant updates because networks were changing all the time.

Endpoint or Host Security

As the world began to understand that sometimes firewalls weren't perfect – that their configurations and instructions included human errors, and malware got through – it became necessary to protect the endpoints: the computers on the LAN. And the protection was not simply antivirus. The malware was sophisticated, often burying itself in the operating system. Computers and their configurations on any LAN are wildly different – they do different things, have different software versions, and such – and malware detection can be very hard to achieve, requiring very heavy CPU processing. Thus, businesses were reluctant to install endpoint protection . . . that is, until it was clear that the malware was on their endpoints and put their businesses at risk. Given the burden, keeping the endpoints safe was essential. The enormous growth of companies like Tanium, Bromium, Sophos, Symantec, and the like illustrates just how quickly businesses have adopted endpoint solutions, in addition to having their firewalls and intrusion detection.

This is a direct result of the strategy "threat/response, threat/response" of the last 30 years. And it's been great. I wish it were enough. But having great firewalls and superior endpoint protection is not enough. These technologies, and their implementation by great engineers, are essential. But what happens when it's all coming down on your head because something didn't work? What do you do? What do you know? What actions can you take without causing further problems? What learnings can you capture?

The chart below shows the increase in sophistication of the threat resulting from the internet and networking, prompting the network security solutions of firewalls and intrusion detection. Further in this category are host or endpoint capabilities. The new threats – about 25 million, in one recent year – were nicely dealt with for about two decades.



Advanced Persistent Threats and Other Scary Stuff

In 2013, something new popped up on the threat "heat map": Advanced Persistent Threats, or APT. This new evolution of the malware universe was really sneaky. It could ride in on normal traffic and not be picked up by firewall / intrusion detection systems. In fact, many endpoint solutions couldn't detect it, either because it was often not launched until an end-user clicked on an attachment in an email or because it could lay dormant until activated somehow. There was a scramble in the market like no one had ever seen. Emerging from this threat was the company FireEye. Struggling for many years, this company's solution was targeted right at the APT; now everybody connected to the internet had to have FireEye. In short order, FireEye's solution became essential.

All of the solutions I've discussed were largely a response to a new threat. The threats were evolving quickly, and vendors responded quickly. To fight these cyber

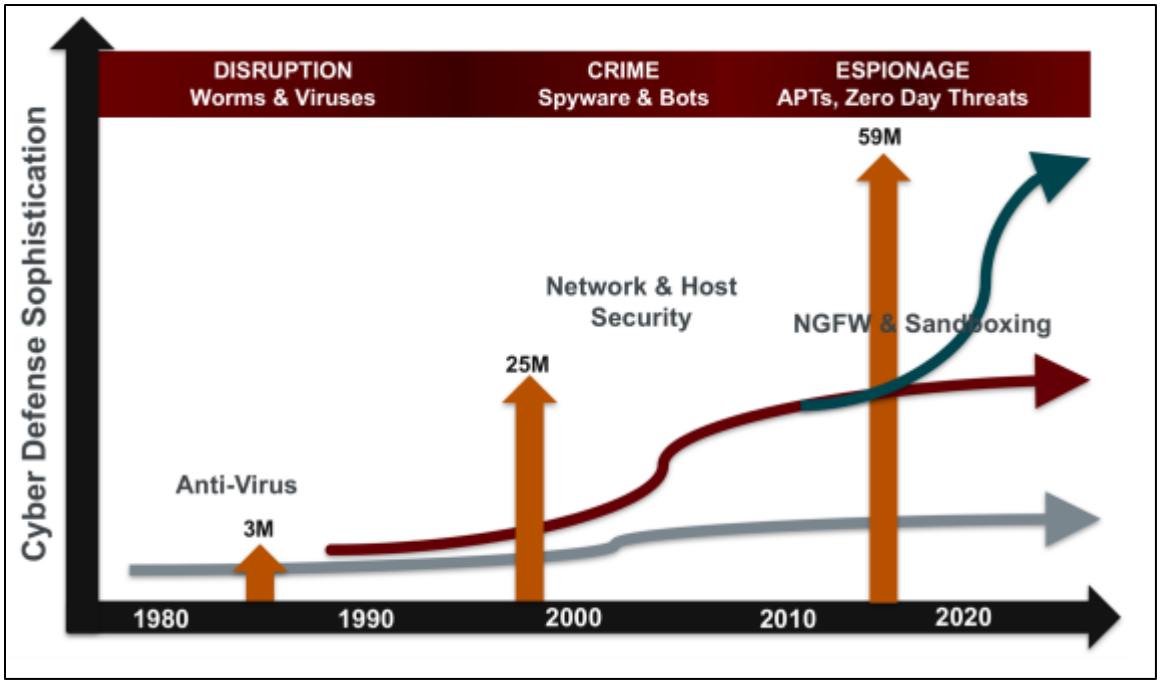
threats, corporations went from spending a few hundred million dollars in the late 1980s to nearly $100 billion in 2016. This was real money, spent by serious and large companies. Yet, it still was only a trickle of total IT budgets, and therefore not really noticed by management. The technology was still run by very sophisticated people, and the implementation of strategies was by the IT departments. It was only in the early 2000s that the title CISO was invented out of the CTO. The Chief Information Security Officer had arrived.

In parallel with network and host security solutions, several new categories began to rise. Firewall management. Vulnerability management. SIEMs. We officially have so many vulnerabilities that there is an entire market dedicated to finding them and alerting security teams. And thanks to Splunk and others, we now have virtual phonebooks of data, updated every day, highlighting suspicious behaviors or indicators of compromise. How we sort out these phonebooks of data has become a debate. Prioritizing what matters in a reasonable time period is challenging.

The Target Corp. Attack

In 2013, something else happened. Target Corp. was attacked. I'll not detail this most infamous attack, but I'll simply say that Target was a very sophisticated company in terms of cyber security. A Fortune 50 company, it had the best technology, the best engineers, and the budget to spend. Yet somehow, the malware found a pathway in – from an innocuous third party at corporate – to ultimately exfiltrate critical customer data from point-of-sales equipment, all connected on the network. The rest, as they say, is history. For me, however, this was an Aha! moment: I saw a new threat from old malware. This threat was the result of just how the network was built and operated. And most seriously, it was a threat for which there was simply no antidote. This threat – or risk, really – was basically a result of how we had built the network.

The chart below shows this next level of sophistication of threats – APTs, Zero Day, the advent of espionage made easy – with the number of reported attacks doubling in the last period of time. While many powerful vendors did things like next-gen firewalls and sandboxing strategies to try and capture the APT / Zero Day threat, the truth and simple math is that if a billion threats hit your firewall, and your firewall is 99.9999% effective, 1,000 got through. And it only takes one to wreak havoc on your business.



I have lived this time period, and invested in many companies dealing with these threats, many of which became the leader in their segment.

From my seat, I see three very distinct phases of cyber-security market evolution: the AV, network and host security, and now we're entering into a third one, for which there is no silver bullet. Each phase can be demarked by how businesses digitize themselves and implement new technologies – whether for connectivity, commerce, or simply ease of management of their business – all while lowering their costs.

Underlying all of this digitization is cheap communications technology. Low costs made it easy to deploy connections throughout an organization, and to make it worldwide. The advent of smartphones in 2007 really turned the connected world on its head. Now everyone was connected to their corporate assets all the time. No longer was the perimeter well-defined, nor the assets well-known – or even where the important data was kept.

> Simply put: There is no cyber solution or solutions that can completely defeat every potential threat in a reasonable, timely, and cost-effective manner.

As adversaries – whether nation-states or business competitors – advanced their threat capabilities, no one could rely on the vendors of the cyber universe to give them the Zero Day solution to all threats.

Just as we have learned to make cars, planes, buildings, and home appliances more resilient against what can go wrong, it is time for businesses to build their networks to be more resilient to the challenges and the disruptions and the threats. I call this new age **Digital Resilience** – not just cyber security.

Digital Resilience

Resilience. It's a common-enough term in modern life, and one that we throw around all the time. *Resilience* is expecting, planning, and surviving an impairment, an attack, or any disruption in normal activities, whereby you can continue operating normally or walk away alive. Humans are remarkable at resilience; our very biology is resilient. We may miss something the first time around, but one or two misses and we start thinking about what can go wrong, and how to avoid it, or how to mitigate the impact. Thinking about what can go wrong turns out to be a really useful learning tool. While I can't document it, I've got to believe that – as quality assurance in the manufacturing age, when everyone thought high quality cost more – we will soon learn that being digitally resilient (operating the network, protecting the assets and the business) is cheaper than the alternative.

Many engineering disciplines teach their students to think resiliently. Being a nuclear engineer from the '70s, this was Job One: defense in depth. Building a machine that could survive a serious defect or impairment – but most important, not harm anyone in the process of the impairment – is pretty hard to do, but not impossible. This philosophy prevailed at the Three Mile Island nuclear-station accident in 1979. Today, I recognize the need for this kind of thinking in the modern digital network and business evolution.

A short elaboration as to why Digital Resilience, and not just cyber resilience: Business today is so dependent on digital technology – like routers, firewalls, and web servers – to get things done, that bad things happen when they fail, even when it's not the result of a bad guy's actions.

Take, for example, July 8, 2015. United Airlines, the New York Stock Exchange, and the *Wall Street Journal* all went dark, and their normal business services were interrupted, all at the same time. The Twitter feeds lit up, postulating that maybe it was a terrorist-motivated attack, or some other mal-intentioned action. It was not. It turned out to be a regularly scheduled router upgrade that went awry. There were probably way more businesses disrupted, but none as visible as these three. This was digital, in my parlance – not cyber, as the term is used today.

How does a resilient strategy apply to our digital networks? Digital networks are relatively new technology. They've been built to be open. They were built fast. And they were built by many people, with many different intentions. And the underlying technology evolved very quickly. So it's not at all surprising that they're not very resilient and, in fact, are quite vulnerable.

Once inside the network, it's common for smart malware to hunt for months and years for its target and essentially not be detected. So, given the vulnerability of the architectures, the imperfection of the implementations, and the phishing (the predominant attack vector today, responsible for more than 90% of the successful events) directed at humans – as it is often said, we are all under attack. Some know it; others do not.

There are three reasons it's time for cyber to be in the boardroom:

1) This level of threat is pervasive.
2) No one is immune.
3) Your company is completely dependent on its digital infrastructure.

Many organizations are moving to this. The National Association of Corporate Directors recently started providing seminars, training, and other information to directors who take the plunge to put cyber strategy on the corporate business agenda. I predict more and more of this, and in short order. While there have been technical courses for engineers and operators for years, to-date managers are rarely introduced to these issues in a framework that is meaningful to their role.

Evolution of Cyber – Costs, Management, Organization

Anti-Virus Days:
- Antivirus, $100, self-managed and self-oversight

Network and Host Security Days:
- Firewalls, Instrusion Detection and Prevention Noticable budget impact but modest.
- Trained network engineers for deployment management
- IT/CTO oversight

APT, ZeroDay, Phishing Days:
- C-level: CISO side by side or under CTO, with specialized skills in cyber security
- Policy and governance for control and cyber security
- Many desparate vendor solutions
- High budget and organizational impact
- Compliance requires highly trained engineers, consultants, and experts

Digital Resilience:
- Senior Management and Board of Directors
- Clear measures, goals and financial impact
- Identified risk, major budget and operational impact
- Strategic deployment for business
- Strategic risk to business

Resilience is a "well practice" strategy. In 2015, McKinsey & Co. published *Beyond Cybersecurity: Protecting Your Digital Business*, which offered the C-suite a way to think about cyber resilience, and steps to take, and nicely couched it in terms that board directors and senior managers need in order to understand.

Directors do not need to understand a Zero Day threat, or even what a firewall is. But they do need to understand the investments they're making, the results of these investments, and the ultimate risk choices they're making, by how the digital side of their infrastructure is operated. Cyber security is a critical element of that understanding. A key takeaway from this important book is that measurement of cyber and its capabilities is fundamental to a modern corporation.

Boards Like Numbers

Boards like numbers. They understand them. It's easy to see if something is getting better or getting worse over time, through the numbers. But what numbers matter in the cyber sense?

Essentially, all cyber vendors offer numbers – signatures for AV, APTs detected, threats measured, and the like. This is interesting for the operations guys, but not for the senior managers and board. It's also not helpful for understanding the strategy with which you are going to manage threats and risk. What matters to a board and management is a measure of the company's ability to respond to a cyber threat, where the assets are, and how a response might be created.

Simple questions, like when the CISO asks for the next $100 million for cyber implementation, how do they know if it was done correctly, or that it even improved things, and how do they convey that result to the board? This *output* of cyber capability is lacking in the industry. Note: This output is not about a particular threat, or a particular technology, or whatever. It should be about cyber readiness, situational awareness, and actions possible in the event that something bad happens. This is much harder to do, and is way more involved than just having the best technology and tools.

However, to begin measurement you need a few basic elements. The first is to simply know how your network is built: what is the state of the endpoints, what are the paths by which endpoints can be reached from the outside or other untrusted sources, and what are the two- or three-hop pathways within your network that leave normally well-protected assets exposed to a lateral attack? Sound easy? It is not. Networks contain millions of elements, configured by many people, over a period of time, for different purposes. People make mistakes. And even compliance standards do not guarantee this knowledge or perfection.

Here's a real-world example to illustrate. You couldn't even begin to install sprinklers in a building if you didn't know how it was built; where the walls, doors, windows, and other infrastructure are; or, in the event of a fire, where the important things to protect are located. Instrumenting a network is just like that. You need to know what is connected to what, what protocol is available over that connection, and what the state of the device is (is it a steel door or a wooden door, for example). Once you have that, you can see the pathways you don't want, and better ways to accomplish a digital task.

These are really basic things. People often have diagrams of their network created with cool drafting tools; however, they are rarely up-to-date, and often have mistakes in them. Have you ever stuck your head in your network engineering manager's office and seen his whiteboard with the network diagram and lots of IP addresses on it? They all do this. Not very practical in an emergency.

Another real-world example suggesting that resilience is a good and proper strategy is the recent WannaCry ransomware threat. This threat wasn't malware lurking in your network – in fact, most networks never even saw it. Rather, WannaCry was a threat that, if it entered your network and found an endpoint that hadn't been properly updated by Microsoft, it could cause havoc. The risk represented by WannaCry existed whether or not you were invaded with it!

McKinsey's resilience concept of "knowing your network" fits here. If, for example, you had a full inventory of all your endpoints – let's say you had five or six million of them – you could ask if Port 445 was open, which would make WannaCry a real risk to your network. In this scenario, what if it reported that 30,000 endpoints were in this condition? Could you easily patch 30,000 endpoints? How long would that take?

Suddenly you're in a repair mode that will take precious resources, and could last for months. The **Resilience** strategy, on the other hand, suggests that you know both your network and the relative risk of its various components: whether an endpoint is reachable, or has critical assets, or both. With this insight, let's say you could reduce the number of endpoints vulnerable to WannaCry from 30,000 to 100. Then you could do something about it, and quickly. That's resilience. Even at my company, RedSeal, we found five endpoints out of 300 or so with WannaCry vulnerability and fixed them within minutes.

In cases where engineers figure out their network, is there really a way to know that they've found it all? What about that old router that was redeployed in last year's new data center, and the instructions weren't wiped from it before it was stood up? How can you know if you've got it all in-hand when a router or firewall can contain hundreds, if not thousands, of lines of instructions?

Knowing how it's built, the state of the devices, and where the traffic can go is Step One, and turns out to be fundamental to building a strategy to defend yourself from that threat that got in. From there, you can diagnose and make changes and improvements. And depending on information, actually war-game it and test your strategy. And, important but often forgotten, actually train people with fire drills.

Can you imagine being a military general planning an invasion without a map of the terrain, the location of the enemy, critical assets available to you, and such? You wouldn't stand a chance. The same is true in network security. In today's world, that might be called a software model of the network. From there, you can measure many things, test changes, and train your troops.

Conclusions

Cyber is a big business, getting bigger – with big budgets, critical policies, and unique risks to the business – so senior management and boards of directors must be involved and lead.

Historically, cyber was a technical issue managed by engineers and similarly skilled people. Now, when the biggest threat is a simple phishing attack targeting anyone with email, every person is part of the cyber solution. It's now everyone's business. From top to bottom, from left to right, everyone must be involved. And therefore, it takes a strategy of policy, technology, personnel, and investment to do it right.

First, digital resilience is not a product. It's a strategy. And it's a strategy that cannot be implemented overnight. Today's networks are complicated, full of disparate vendors' products, and were built by many folks over a long period of time with the strategy of openness in mind. Networks need to be open, and will be open even in digital resilience. It starts with understanding what you have, where the assets are, and how it is operated.

Second, if you know where your jewels are, you know where you need extra control and policies to manage that access, control, and security. Just like in life, not everything in your network is equal. Knowing what matters, and where it is, is huge in terms of prioritizing what to do first. Knowing where you are vulnerable would impact this thinking, too. So, just "doing" is not sufficient. Doing smart, verifying what's done, and measuring the outcome is critical.

Third, know which measurements matter. Most everything is measured. However, what's put in front of the decision makers, like the board, is consolidated. And knowing which measurements matter is critical. If you can't measure and see everything on your network, there's no way you'll provide the right or the appropriate measurements. You must have that visibility.

Fourth, visibility is hard. That map of the engagement for a battle doesn't come from thin air. It shows carefully determined, checked, and verified data. Your network is exactly the same. The machines that run it are sophisticated and highly engineered – not for the standard technician. Automation turns out to be key to grasping all that your network is. There are vendors in the market that provide elements of this visibility. But no one has a complete solution. It'll take more than one vendor.

Fifth, your network is a capable resource in the path to resilience. Like a well-constructed and -maintained building, your network is the foundational element upon which resilience must be built. Don't short-change it or fail to maintain it. Make the investment, measure the output, and just like human immune systems, continue to adapt and strengthen.

No doubt there will be more big-news cyber attacks and crimes that impact our world. Like everything else in your business, you need to manage your cyber readiness and capabilities. And to manage it, you need to measure it. To measure it, you must be able to see it, analyze it, and understand it. And you should start today,

because whether you know it or not, you are under attack. It's only a matter of time before you'll be faced with managing the situation.

About Ray A. Rothrock

Ray A. Rothrock joined RedSeal as CEO in February 2014. **[*Ed. Note:* RedSeal has been selected as a 2017 FiReStarter company, and you can meet Ray at FiRe.]** Prior to RedSeal, he was a general partner at Venrock and one of RedSeal's founding investors. At Venrock, he invested in 53 companies – over a dozen of which were in cybersecurity, including Vontu, PGP, P-Cube, Imperva, Cloudflare, CTERA, and Shape Security. He is on the board of Check Point Software Technology Ltd., an original Venrock investment, and Team8.

A thought leader in cybersecurity, Ray was a participant in the White House CyberSecurity Summit held at Stanford University in February 2015. A sought-after speaker, he has been a featured panelist at this year's SXSW Conference, the lead moderator for the CyberSecurity Panel at the Milken Institute Global Conference, and a speaker at the 2017 NACD Global Board Leaders' Summit.

Ray holds a BS in Nuclear Engineering from Texas A & M University, an MS in Nuclear Engineering from the Massachusetts Institute of Technology, and an MBA with Distinction from Harvard Business School. Ray is also a member of the Massachusetts Institute of Technology corporation board.

I would like to thank Ray for bringing our members to the leading edge of what can, and cannot, be done by the tools of modern cyber war; and to thank Editor-in-Chief Sally Anderson for putting all of these thoughts into perfect shape.

Your comments are always welcome.

Sincerely,

Mark R. Anderson

CEO
Strategic News Service LLC Tel.: 360-378-3431
P.O. Box 1969 Fax: 360-378-7041
Friday Harbor, WA 98250 USA Email: mark@stratnews.com

CLICK HERE TO SHARE THIS SNS ISSUE

To arrange for a speech or consultation by Mark Anderson on subjects in technology and economics, or to schedule *a strategic review* of your company, email mark@stratnews.com.

We also welcome your thoughts about topics you would like to suggest for future coverage in the SNS Global Report.

For inquiries about **Partnership or Sponsorship Opportunities** and/or SNS Events, please contact Sharon Anderson Morris, SNS Programs Director, at sam@stratnews.com or 435-649-3645.

INSIDE SNS

Please visit www.stratnews.com/insideSNS for:

- Photo galleries of FiRe and other SNS events
- FiRe videos
- SNS iNews®
- The SNS blog, "A Bright Fire"
- The SNS Media page
- SNS FiReFilms
- Subscription rates and permissions
- About SNS and About the Publisher

UPCOMING SNS EVENTS

"BREAKING THROUGH"

Register now for FiRe 2017
The 15th annual Future in Review conference
October 10-13


Credit: Kris Krug (L) and David Morris

Returning to the beautiful
Stein Eriksen Lodge Deer Valley
Park City, Utah

www.futureinreview.com/register

WITH GREAT APPRECIATION TO:

Our Global Platinum and FiReFilms Partner:

Global Platinum Partner:

Deloitte.

Global Gold and FiReFilms Partner:

ZIONS BANK

Global Silver Partner:

accenture
High performance. Delivered.

Global Bronze Partner:

Microsoft

and Focus Channel Partners:

otonexus MEDICAL TECHNOLOGIES

KINETA Translating Science | Transforming Lives

VENAFI

haydale

HARRIS+HARRIS GROUP

illumina

... for their Partnership and Support of SNS events.

ADDITIONAL SUPPORTING ORGANIZATIONS

parkcity.institute

FiReFellows Sponsor:

ZIONS BANK

and FiRe Academic Partner:

Where's Mark?

• On October 10-13, Mark will be hosting the 15th annual Future in Review conference at the Stein Eriksen Lodge in Park City, Utah. To register for FiRe 2017, go to www.futureinreview.com. • On November 15, he will be keynoting the Radar Co. annual conference in Stockholm; on November 16, he will be speaking to members of the Founders' Alliance there. • And on December 7, he will be hosting the SNS Annual Predictions Dinner in New York, at the Lotte Palace Hotel.

ISSN 1093-8494