Published in Authority Magazine

Get started Sign In

Jason Remillard

Jul 2, 2021

15 min read

Listen

Ron Indeck of Q-Net Security: 5 Things You Need To Know To Optimize Your Company's Approach to Data Privacy and Cybersecurity

An Interview With Jason Remillard

Search

Jason Remillard

67 Followers

Leading the charge in bringing data privacy as affordable, deployable and realistic solutions that every business owner can take advantage of

Follow

More from Medium

Carlo S...

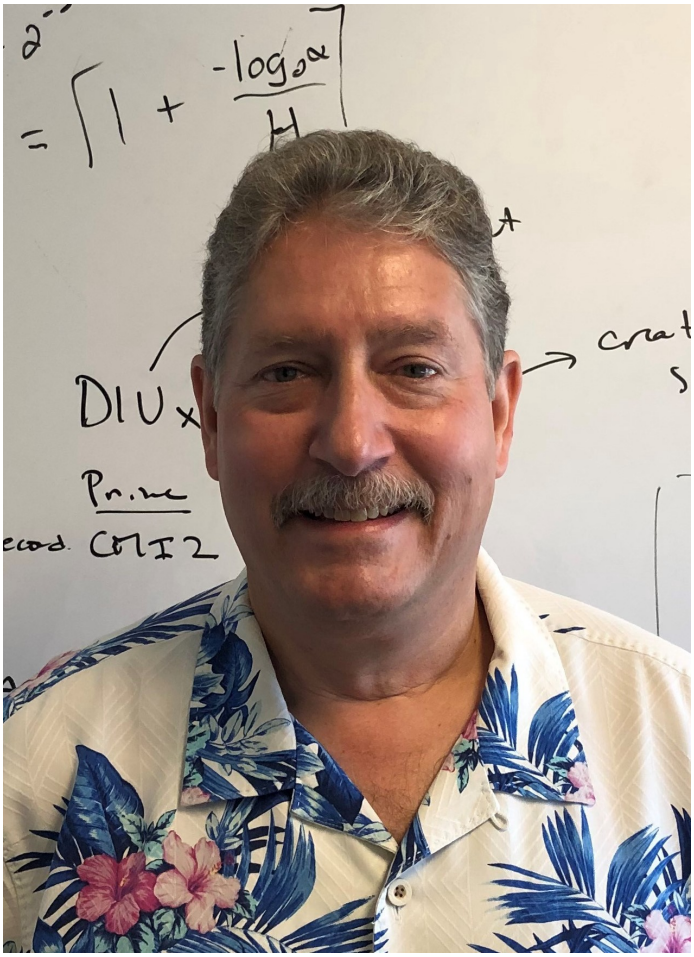
My learnings with Exordi

Recurate

Get To Know: Sumita...

Ratpacer

Are Things Better With



The very first step in improving cybersecurity is to become informed! As I mentioned before, it's not a good strategy to pretend that cybersecurity breaches will never happen, or

Amazon,…

Yogesh…

Perotium—who is called the…

Help Status Writers Blog
Careers Privacy Terms About
Knowable

> they won't be very damaging if they do. Learning about the current state of the technology, and what options can be achieved easily is the first goal in better protecting oneself and one's company.

As *a part of our series about "5 Things You Need To Know To Optimize Your Company's Approach to Data Privacy and Cybersecurity", I had the pleasure of interviewing Ron Indeck, Ph.D.*

Ron Indeck, Ph.D. is the CEO of Q-Net Security, an innovative cybersecurity company based in St. Louis. Prior to joining Q-Net Security, Dr. Indeck served as President, CTO, and Founder of VelociData, a technology spin-out

delivering accelerated decisioning to global corporations. Before forming VelociData, Ron founded and was CTO to Exegy, a firm that enables over $1 trillion in trades daily. At Washington University in St. Louis, he was the Das Family Distinguished Professor and Director of the Center for Security Technologies. His security technology has been incorporated into roughly half of the card readers in the world. He has published more than 60 peer-reviewed technical papers and been awarded more than 75 patents; been named the Bar Association Inventor of the Year; and served professional societies in various roles including IEEE Magnetics Society President.

Thank you so much for joining us in this interview series! Before we dig in, our readers would like to get to know you. Can you tell us a bit about how you grew up?

I grew up in the mosquito-filled tundra of Minneapolis, Minnesota, as the fourth of four boys. To this day, we still have no idea how my mother survived us all! Education was extremely important in our home, curiosity was encouraged, discussions were demanded, and advanced formal training was expected. All four of us have advanced education and degrees. This has carried on to our children as all of them have doctorates, which hopefully is part of a positive life attitude and not a burden. Science and math, or STEM, were the strong drivers. I recall being given a chemistry set for my birthday and I did many fun experiments from making color changing salts to indicate humidity, to (un)controlled explosions. Did I mention how we have no idea how my mother survived our childhood? I also remember taking things apart to see how they work even though I frequently had parts left over after putting them back together. This set

me on a path to pursue engineering as a career, teacher, and passion.

Is there a particular story that inspired you to pursue a career in cybersecurity? We'd love to hear it.

I was raised in the '60s and while we may think back on the drugs, sex, and rock-n-roll counterculture, the Vietnam War, or the nuclear-fueled Cold War, there was another remarkable thing happening during that time — President Kennedy set up a mission to the moon. This moonshot, along with the Mercury, Gemini, and Apollo programs, created an amazing and awe-filled time where anything could be accomplished. I recall having the pictures of all the astronauts on my wall, photos, and models of different rockets in my room, and very closely following many of the activities associated with the space program. I actually wanted to be an astronaut, even though I was told my need for glasses meant I could not be a pilot.

Anyway, the United States reaching a dramatic high with the lunar landing (which I watched alone on a small black and white TV), became the inspiration for me to ultimately go all in on engineering rather than other sciences or medicine.

Can you share the most interesting story that happened to you since you began this fascinating career?

What's in a word? To most of my colleagues, "noise" is a random process that is always different every time you measure it. Such random processes give people an understanding of what can and can't be done. As an example, Claude Shannon provided us with a view into how much information we can put into a communications channel in the presence of random noise. My research led me to investigate a communications channel in which we put the data to rest in the middle — the magnetic recording channel. For decades, the noise in this channel

had been viewed as random and no different than the processes caused by such things as temperature-induced variations. With my physics background, we started to look at the sources of magnetic recording fluctuations and discovered that a large portion of the “noise” was repeatable. This was fascinating for me as any repeatable signal can be engineered down or even removed entirely. Additionally, it can provide insight into how to engineer a better channel (the recording medium and recording process) to get more information through this channel. For some years, we presented data that demonstrated recording media contained a large component of “repeatable noise” owing to material nanostructure. However, most in the industry could not believe the results and thought we got the experiments wrong, even scoffing at us in professional conferences. As I look back, I think many were simply unable to move past their narrow understanding of the word “noise.”

Yes, words matter, even in science!

None of us are able to achieve success without some help along the way. Is there a particular person to whom you are grateful who helped get you to where you are? Can you share a story about that?

Thankfully, I have been blessed to work with a multitude of really talented and driven colleagues through my career and I am deeply indebted to them all. That said, there is of course a particular person that stands out having helped me get to where I am today — my wife.

This is not a trite attribution to her but rather a recognition that I have taken a rather unusual professional path through academia, to research, and on to entrepreneurship. And she has supported me the entire way. She buoyed me numerous times when a stable future was quite uncertain. She guided me through difficulties

when those managing things got in the way of success. She was always supportive as we started on risky new ventures. She even took charge of our young family as we headed to Japan, a country we knew little about, including the language. I could not be where I am without her support and guidance. She is even my best friend.

Are you working on any exciting new projects now? How do you think that will help people?

Definitely. Q-Net Security is committed to securing the nation's critical infrastructure. I think we've all seen just how fragile pieces of that infrastructure can be (electric grids, gas pipelines, and even food!). Our primary technology, the Q-Box, is a hardsec device that can dramatically reduce the risk to those organizations. While we aren't ready to disclose what is coming soon at Q-Net, we can confidently say that there are new solutions in the works to

help both governmental and commercial customers to better protect themselves.

What advice would you give to your colleagues to help them to thrive and not "burn out"?

Well, it may sound somewhat straightforward, but I would suggest that you find something that you enjoy doing! Beyond that, I would also say not to immediately give up on something, even if it is a little difficult at first. Many people can be burnt out when they are working on something in which they don't have any interest. But it's also the case that if you don't work through and get better at something that was originally difficult, you might not feel very fulfilled in the end. Working solely for a paycheck has never been my motivation, and finding something you're passionate about will often lead to more satisfaction!

Ok super. Thank you for all that.

Let's now shift to the main focus of our interview. The Cybersecurity industry, as it is today, is such an exciting arena. What are the 3 things that most excite you about the Cybersecurity industry? Can you explain?

Well, as the CEO of a cybersecurity hardware company, I am of course going to mention hardware devices! Hardware security, or hardsec, is a new and innovative way of thinking about security devices. In today's world of agile development and rapid patching, it's easy to assume that software is the solution to every problem. But really, the idea of hardwiring security into a device, which cannot be changed, modified, or circumvented, is a new idea and one that we certainly are very excited about at Q-Net Security. This enables us to deliver solutions that are provably secure, which is something that software cannot do.

In that vein, the second item that I'm

excited about is the idea of "protection" being a really viable strategy in cybersecurity. Over the last decade or so, we've seen a shift in thinking that "detection," i.e., recognizing when someone is attacking your system, is the right way to approach security. That is to say, if you can tell when someone is attacking you, you can adapt and modify your system to stop them. Unfortunately, the pendulum swung a bit too far in that direction, so it's exciting to see it coming back around to the idea of protection — stopping someone *before* they actually breach a system. I think there is great work being done in that arena, by our team and others in the industry.

And finally, I'm just excited that cybersecurity is coming into the public eye a bit more. Obviously, there has always been (since the advent of computers at least), efforts toward securing them. But I think recent events, like the Oldsmar Water, Colonial pipeline, and JBS

hacks, have really driven home to the broader public that there are really important systems that are run by computers, and we ought to be investing in the best technology to protect those systems. I'm certainly not excited these attacks have occurred, especially since they could have probably been mitigated somewhat by investment in new technology, but I'm trying to find a silver lining here. I'm glad the industry is finally being taken with increased seriousness.

Looking ahead to the near future, are there critical threats on the horizon that you think companies need to start preparing for?

Absolutely. We're increasingly seeing zero-day exploits and more sophisticated cyber attacks. Moreover, we're also seeing that larger and more critical companies and organizations (like utilities and other critical infrastructure) are now being targeted by very organized

groups of cybercriminals. I think there is a temptation to assume that, “oh, there have always been hacks, and it’s just a fact of the modern era,” but truly, things have gotten more dangerous. It would be a mistake to assume that our existing efforts will continue to be enough to adequately protect us.

Do you have a story from your experience about a cybersecurity breach that you helped fix or stop? What were the main takeaways from that story?

It’s of course exciting whenever you’re able to prevent something that has the potential to cause real damage. Unlike the movies, we rarely have the opportunity to be actively working on a breach as it happens, but the work we do during and after a breach to make sure it doesn’t happen again is very fulfilling.

What are the main cybersecurity tools that you use on a frequent

basis? For the benefit of our readers can you briefly explain what they do?

As a technology innovator, Q-Net Security designs and builds hardsec tools. That means that we actively create hardware devices that are capable of preventing attacks on systems. Our solution uses the highest grade of encryption (AES-256 GCM), but we go even further than that by actually changing the encryption key used up to once per packet or about a million times a second. It means every piece of data that flows through your network is protected by a new, very hard-to-crack password. We can provably show it would take billions upon billions of years to break through our encryption.

Of course, we use other tools as well in our day-to-day work! We maintain secure VPN connections into our network, enforce two-factor authentication, and operate strong

and well-maintained firewalls. Our products go through extensive certification as well, and we constantly update and check our systems to make sure they are properly maintained.

How does someone who doesn't have a large team deal with this? How would you articulate when a company can suffice with "over the counter" software, and when they need to move to a contract with a cybersecurity agency, or hire their own Chief Information Security Officer?

Well, while we certainly advocate for everyone to be aware of security issues, we understand it often seems like something that smaller companies "can't afford to bother with." To tell you the truth though, every company has the potential to be vulnerable to a cybersecurity breach. And just as you are willing to pay for insurance to protect your company against fire, liability, or

other damages, you should understand that an investment in cybersecurity is just that — insurance. The costs of a cyber breach are real, everything from actual lost data to lost productivity and time as things are repaired. We're seeing such an uptick in ransomware recently and that is something that can impact any company.

At the very least, even the smallest of businesses (and individuals) should backup their systems, so that they can restore them if a breach occurs. Beyond that, companies should set up basic firewalls and password systems. Often, you can hire a network professional to do a one-time set up, which will get you started. But after the company grows beyond just a very few people, you should consider bringing in full-time IT expertise. It also depends on the potential for damage! A hospital, where a computer failure could result in physical harm to patients, is under

a lot more threat than a restaurant, for example. Q-Net Security is helping since our products are plug-and-play, easy to drop-in, and no patching or updates are needed for the life of the devices.

As you know, breaches or hacks can occur even for those who are best prepared, and no one will be aware of it for a while. Are there 3 or 4 signs that a lay person can see or look for that might indicate that something might be "amiss"?

Often, the hacks that go unnoticed are ones where the attackers are trying to exfiltrate (steal) data. So it could be some form of corporate espionage, or just people trying to steal personal data to sell on the black market. Ransomware attacks, on the other hand, rely on hackers intentionally contacting the victims for ransom, so those are more obvious.

In the former case, however, the

obvious threats are things like password changes. Good systems will notify their users when their password is change (never ignore that!). Or, you might see an increase in phishing emails, or a change in their sophistication. IT departments often monitor emails and should warn users of particularly convincing emails. There are more less-obvious signs, but they are something that a dedicated team and network monitoring system would catch — not a layperson.

After a company is made aware of a data or security breach, what are the most important things they should do to protect themselves further, as well as protect their customers?

Most companies should consider calling a specialist. There are companies that specialize in just this sort of thing. Some of them will even take over negotiation for you during a breach, such as during a ransomware

attack. After the breach is resolved, companies should investigate and audit their processes. How quickly were systems restored? Were backups in place? These answers may guide to where the most vulnerable parts of their system existed.

Outside of the merely technical steps, a company should probably meet with its public relations and legal teams to determine what kind of statements they must and should make to notify stakeholders that were affected by the breach. While no one wants to be the bearer of bad news, attempting to hide a breach is likely to come back with a very negative outcome in the future!

How have recent privacy measures like The California Consumer Privacy Act (CCPA), CPRA GDPR and other related laws affected your business? How do you think they might affect business in general?

Yes, privacy measures like that have certainly made the requirements for protecting customers much more explicit and well-defined. That means fewer companies in general are able to ignore cybersecurity issues, and means they need to have a plan to deal with breaches by law. One of the lesser-known laws that is actually quite relevant is California Rule 21, which requires devices to have cybersecurity protections in place. This means that every generator less than 1 MW in the state needs cybersecurity protections, and that has really driven home the need for hardest devices like ours.

What are the most common data security and cybersecurity mistakes you have seen companies make?

First and foremost, many companies assume that “it won’t happen to them.” It’s a form of a gambling with your company’s fortunes, and while it may pay off, it’s a dangerous game to

play. All companies are targets for cybercriminals, because all companies have business they want to accomplish. If a ransomware attacker can stop you from doing that business, then they can blackmail you for money.

Another and related problem is companies acknowledging that they may be at risk for an attack, but assuming that the cost of fixing or repairing the damage from the attack would be cheaper than protecting from it today. That is very rarely the case, especially since the costs of an attack extend far beyond just the material cost of replacing computers. There is real reputational damage that can occur. And, consumers are less and less tolerant of bad practices with regard to cybersecurity — even up to the point of holding the company liable for legal negligence.

Since the COVID19 Pandemic began and companies have become more dispersed, have you seen an

uptick in cybersecurity or privacy errors? Can you explain?

Oh certainly. Any time companies are moving en masse to more remote and networked work, it means more potential for mistakes. When a company sends data over the Internet to and from workers' homes, it is risking that data being read. VPNs mitigate that risk, but don't go far enough to ensure true encryption.

Ok, thank you. Here is the main question of our interview. What are the "5 Things Every Company Needs To Know To Tighten Up Its Approach to Data Privacy and Cybersecurity" and why? (Please share a story or example for each.)

1. The very first step in improving cybersecurity is to become informed! As I mentioned before, it's not a good strategy to pretend that cybersecurity breaches will never happen, or they won't be very damaging if they do. Learning about the current state

of the technology, and what options can be achieved easily is the first goal in better protecting oneself and one's company.

2. Secondly, companies need to be aware that there are numerous approaches to cybersecurity. It's not the same old game where you simply tell people to have better password hygiene and you buy an off-the-shelf firewall. Hackers and cybercriminals are more sophisticated than ever before; our responses need to be more sophisticated as well.

3. Carrying on from that prior point, it's important to note that there are different solutions that are appropriate for different situations. We often discuss the difference between "IT" and "OT," or information technology vs. operational technology. Those terms may seem opaque and technical, but the point is that there are different aspects of your business that require different protections. The machines on the assembly line in a factory need different protections than the computer terminal that the office

uses to check its email. Many CISOs understand this, but growing companies sometimes think one approach will work for everything.

4. Hardware, hardware, hardware. I cannot stress enough that software security is vulnerable, and truly dependent on the abilities of those who maintain it to develop updates constantly in response to new threats. Using hardware obviates the need for updates and costly maintenance, and lets you make a strong solution from day one.

5. Finally, I'd caution executives to try to cut through some of the "techno-babble." Because of the growing nature of the cybersecurity industry right now, there are dozens of new cybersecurity startups that are aiming to solve these real problems using sophisticated "learning algorithms." But these primarily boil down to reactionary detection systems that may limit attacks without fully protecting your systems. The methods of the past rely on

> detection and the future lies with protection, along with stopping hackers before they strike.

You are a person of enormous influence. If you could inspire a movement that would bring the most amount of good to the most amount of people, what would that be? You never know what your idea can trigger. :-) (Think, simple, fast, effective and something everyone can do!)

I would suggest that we really need to consider computing from a new angle. Obviously, many of our lives have been improved by general-purpose computers in so many ways over the last few decades. In the span of fewer than 30 years, we've moved from computers being primarily a feature on college campuses to having a computer or multiple computers in most homes. The flexibility of those devices to do anything and be anything is great, but we can't forget that much of the

world, and our infrastructure, works on dedicated systems. That includes some that haven't been updated in years. We can embrace these systems for what they are, specialized hardware, and that will really improve security.

That's a pretty technical wish! I suppose generally, I would want to inspire people to just be a little more conscious of security in their day-to-day lives. Your data is important to you and treating it with care can really pay off.

How can our readers further follow your work online?

By following Q-Net Security:

- Website — www.qnetsecurity.com
- LinkedIn — https://www.linkedin.com/company/qnetsecurity/
- Facebook — https://www.facebook.com/qneti

nc15

- Twitter — https://twitter.com/qnetsecurity
- Email — info@qnetsecurity.com

This was very inspiring and informative. Thank you so much for the time you spent with this interview!