accenture

CYBERSECURITY WEBCAST – JUNE 15, 2017

VIDEO TRANSCRIPT

Thank you for joining us today. My name is Kevin Richards.

I'm going to share a secret with you today that every cyber-attacker doesn't want you to know.

In fact, it is the single most effective cyber-attack in use today – and by effective, I mean really effective – I'm talking – at times is 80-90% effective. It's simple, it's fast, and – oh – did I mention it's actually pretty cheap?

[Kevin: look around]

Here it is. [Kevin: show Starbucks gift card]

With this, I can bypass just about every firewall, learn the passwords of countless millions, and circumvent seemingly every control your Security team can configure across your enterprise – for which I am more than happy to buy you that next latte.

The approach is pretty simple – let me set the stage… You're a recent college grad – a fact that we easily picked out of your social media activities – working for a client that we want to attack. You get an email – let's say from your recruiting team – saying, "we are expanding our campus recruiting next year. We've identified [your alma matter] as a campus of choice based in no small part on your strong performance. Can you please take a few minutes to complete this survey? It will help us target our messaging to attract the best and brightest." and then it closes with, "we know this is outside your normal

closes with, "we know this is outside your normal job duties, so, here's a small token of our appreciation" – which is a link to a $5 coffee gift card. It is authentic – and of course you would love to elevate your alma matter. So, you click on the "Take Survey" button, fill out the survey, and get your gift card – off you go for your latte! What you didn't know was that there was malicious software being downloaded onto your computer in the background that is now providing a range of access to corporation – looking like it came from you. It's brilliant in its simplicity.

Today, I'm going to reveal three basic facts about cybersecurity that will allow organizations to dramatically improve their performance by adopting a completely new approach to protecting their most valuable assets.

1.) While we've made amazing progress in protecting our companies, our employees and our families, we still have a fair amount of room to grow,

2.) We need a new way of thinking about the cybersecurity problem – because the way we're approaching it now just isn't working,

3.) This is a solvable problem when we break the problem into manageable chunks.

So, lets dig deeper into these three…

Number 1 – we're making progress, but…

We’ve never had more visibility to cybersecurity – with corporate leadership or even at a personal level. We’ve all seen the headlines – think back to just a few weeks ago with the latest RansomWare attack ... WannaCry.

In just a few hours, millions of files were encrypted and locked on hundreds of thousands of systems through a piece of malicious software – with a ransom note: “pay $300 in BitCoins and get your files back.” It impacted thousands of companies – and some quite critically.

Or maybe you’ve received a letter from your bank, favorite retailer, or insurance provide apologizing for inadvertently disclosing your personal information.

At a Board level, Cybersecurity ranks within their top 3 critical risks – up there with financial risks and reputational risk.

And with that concern, we are dumping more money into Cybersecurity than ever before. In 2016, we as a market spent over $80B on Cybersecurity; by 2020 it is estimated that number be north of $120B annually.

Unfortunately, even though we’re spending big, we’re still losing big – and it’s not just personal inconvenience, breaches are costing us a lot. By 2019, it is estimated that breaches will cost companies over $2 trillion – that’s trillion – with a “T”… at the pace that we’re going, that could top $120T in losses over the next 15 years.

The crazy thing is that even though we keep spending more, we’re not solving the problem – or even slowing it down… We need to understand this a bit more.

Being Accenture, we did what we do best, we started talking to our clients. We interviewed 2000 companies in 15 countries and 12 industries; all were $1B in revenues or bigger, and we talked to the top cybersecurity person within their company. It was a simple set of questions to gauge their sentiment and capabilities. Their answers were fascinating.

As true warriors, the Cybersecurity leaders billowed with confidence: 75% were confident in their ability to protect and defend their enterprise – bringing demonstrable value to their corporate shareholders. Further, over 70% felt they had an enterprise-wide culture that embraced and embedded cybersecurity thinking.

The respondents highlighted significant Board interest, effective investments in network and endpoint technologies, detailed advancements in digital identity, and certification to compliance frameworks and standards. All good things.

As we pushed a little harder, though, the confidence began to fade. Roughly two-thirds (66%) of respondents acknowledged that they don’t quite know how or when cyberattacks will affect their company, and when the attacks are successful, it can take literally months for over half of the respondents to detect the attack. Further, only 37% were confident in their ability to monitor for breaches – meaning 63% - or nearly two-thirds – were not confident.

Then, the $2 trillion question, how often do companies get breached? We should qualify this question just a bit… In our world of connected everything across the Internet, there are literally hundreds of thousands of “attacks” that we’d best characterize as “noise”… These are easily blocked by our common technologies – firewalls, encryption, and the like. With that in mind, we asked the respondents to only consider focused, targeted style attacks – as opposed to the random noise.

Now that we’re properly calibrated, I’ll remind you of the question: how often do companies get breached? On average, the respondents acknowledged they were experiencing 106 targeted attacks annually. Of those, 32 were successful annually.

That’s basically 1 in 3 attack attempts being successful in getting through the respondent’s defenses… or 2-3 breaches per month for the “normal” large enterprise. If we take some other market data that the average breach costs a company $4 to 5 million each, this is suggesting that it is costing companies $8 to 10 million per month due to cyber attackers.

To be honest, we were stunned. We kind of all suspected it, but having the data in black and white was staggering. In the face of this new information, it's easy to see why cybersecurity confidence starts to fade quickly…

So, we have what clinically can be called a "conundrum"…

We're spending more, it's costing us exponentially more, and it doesn't seem to be getting any better…

Which brings me to my second point – there must be a better way…

In many respects if feels like a lot of our security programs look like this:

We started out with great intentions and amazing capabilities but it hasn't worked out over time. Budgets get reduced, it's hard to retain top talent… things simply start to age, and we had to get – well – creative in our defenses.

This, by the way is a genuine image taken from a real location – not a posed image for the camera … I LOVE the zip tie…

[Kevin Move to New Position 2]

I think it's safe to say – and I'm guessing you'd agree – that we need to something different, but which way to go?

It may make sense – and hopefully be helpful – to see how we got here. Our common thinking on cybersecurity goes back thousands of years using a term called "defense in depth".

The notion is that the most important or valuable items – the King and Queen, the people, the money, the jewels – are in the center of a cascading series of protectionary walls – each with their own set of obstacles and controls that the would-be attacker would need to overcome to be able to steal the valuables.

This mimics a traditional approach to cybersecurity.

The data center goes here in the top middle section; your web site and other Internet facing apps go inside the outer wall; You've got your "throttle" points – i.e., firewalls, which are the doors. We put a lot of technology – let's call them controls – all over the place.

It's a little dramatic of an example – maybe a little simple, but this is just how we built network security – "back in the day"… It works great so long as all the important stuff stays on the inside, we can keep the only way in or out through the one front door, and we have the ongoing investments to maintain the environment.

Coming back to June 2017, unfortunately, our enterprise doesn't look like this… With the liquid workforce, mobility, smart phones, tablets, WiFi and Internet everywhere, cloud first – these have a dramatic impact on our defenses. Now the bricks in our highly fortified walls look like this:

Our original strong and solid walls are now riddled with openings that attackers can easily drive right through.

Remember, we've intentionally opened access to support worker mobility, partner relationships, and improved customer experiences. Enter in wearables, connected vehicles, and the interactive connected home, and sometimes you can actually see straight through the holes.

The notion of protecting our enterprises through bigger and better walls simply won't work – putting the genie back in the bottle – technologically speaking – isn't the right answer.

Our security programs are running to keep up with the Digital explosion – the technology is advancing faster than the security program, and it appears that there is still a change of thought needed

If we go back to our research – 58% of respondents – so over half – say that if they were given more budget, they would spend it trying to fill gaps in their network security. Over half would spend extra money on an area that we've already concluded isn't working..

Then… where did we go next? Enter in "Compliance".

We've had an over reliance, and unfortunately, a misapplication of using compliance as a surrogate for security. Looking at numbers, maintaining compliance continues to be the single largest cybersecurity expense. It is understandable – auditors get a direct line to Board of Directors. The fear of fines or material audit findings drives a whole range of avoidance behaviors. Don't get me wrong, I bear no ill will towards compliance programs – I am quite thankful for them. Compliance management might be the single largest expense for the security program, but it is also the single largest motivator for increasing security budgets – fear of compliance gaps has fueled a significant portion of the security industry.

My intention here is to drive an understanding of difference between compliance and security, and to raise the understanding of the content of an audit report – what it is really saying – so executives have clarity.

Again, I am a staunch believer in audit – meaning, "we wrote down a plan on how we want to manage our environment that meets a wide range of requirements" – then "did we do it?" It is a meaningful and material quality function for an enterprise – think "checks and balances."

Unfortunately, many oftentimes confuse compliance with security. They are very different, and relying on compliance to actually protect the business has caused some devastating consequences.

Here's a quick example.

[Kevin, Move to New Position 3]

Let's think about the 5 biggest retail credit card breaches over the last few years. One thing they all had in common, was that they were all PCI compliant – PCI is Payment Card Industry – the group that creates requirements for protecting electronic credit card transactions. Please note that I think the PCI Data Security Standard is actually quite good. My caution with PCI as a security construct – and the same lies in many other audit construct for that matter – lies in one phrase: "audit scope". Audit scope is a practical "fence" that is put around those areas and items that will be included in the audit. And before I get the hordes of auditors yelling at me, I completely understand the operational construct around the need for scoping – it makes the audits faster, and doesn't over burden an entire organization; and I understand the sampling approach, which if done properly, the results can be statistically relevant for the review. Yes – all true. The problem lies in largely in the presentation of the findings, and then the education of executives on what that report is saying.

Let me give you an example

[Kevin Move Back to Position 1]

Here's my fortress.

The box on the top represents the scope of the PCI audit – that's the area of servers and infrastructure supporting this nation's eCommerce environment.

We put in all the technology controls, passed the audit, and received our compliance report. Great.

The next day, bad guys storm the fortress – a successful cyber attack. Invariably, there's a conversation with the CEO – "How did this happen? I just got a report saying passed – compliant… and today we're a headline… What's going on?!?"

This illustrates the exact issue with "scoping".

The PCI audit didn't look at *all* of the ways an attacker might try to penetrated the enterprise, it only looked at the systems that were relevant to the electronic credit card management process. The rest was deemed "out of scope". It never looked at this drainage pipe at the other end of the fortress.

The conversation to the CEO is, "yes, you're compliant, but that didn't mean your whole kingdom was protected."

This is a sizable challenge for organizations. Maybe there are several different audits that take place – I guess you might be able to "stitch together" a complete view. Unfortunately, with declining budgets for all departments, no one is, and we end up with incomplete pieces of the puzzle.

We've seen the numbers and now understand how we got here, let me reveal the third item for you, a better path forward.

The bad guys want you to think that this is still a hopeless dilemma, that with enough time and energy they'll inevitably be successful. I'll submit that we may never have perfect security – but this isn't about submission, this is a solvable problem. Success isn't measured in the absence of risk; it is measured by maximizing successes in the face of risk. Here are six things every security leader can do to materially improve their security effectiveness.

Number 1 - LEAD FROM THE TOP by materially engaging with enterprise leadership & improving the board's cyber literacy.

Many people tell me they lead from the top and that they have regular interactions with their Boards. The reality, though, is that many of those interactions are perfunctory or superficial. Are the meetings once a month or once a year? Do they include a meaningful exchange of ideas or is it simply a "report out" on past efforts? Are you expressing your true concerns about the enterprise, or are you holding back out of fear of losing your job or getting someone in trouble? I'm not suggesting that we run around screaming "the sky is falling" but the CISO needs to be the foremost expert on cybersecurity. The Board and C-Suite need to hear any concerns – it's not just a job, it's our duty.

NUMBER 2 - MAKE SECURITY EVERYONE'S JOB by fostering a culture of cybersecurity & prioritizing training of all employees.

If a $5 gift card is the most effective cyberattack, its kryptonite is knowledgeable employees. The most effective firewall is a human firewall – educated, impassioned, prepared. Unfortunately, only 17 percent of the survey respondents said given additional budget they would spend it on better preparing their front line staff for defence. This is our secret weapon. Trained properly, every employee can make a difference – and stop attacks before they start. Think back to my opening example – if I simply don't click on the link, the attack never happens.

NUMBER 3 - PROTECT FROM THE INSIDE OUT by prioritizing protection of organization's key assets.

If I can use a bit of a sporting analogy… in football – with equally matched teams – the offense has the advantage: it *knows* the play. The defense must guess and react once the play starts. We have a huge advantage to any attacker. We know (or at least should know) our key applications; we know where our important data resides; we know our employees and who should be accessing our applications. The attackers need to figure out all of this. We have the upper hand and can decide in advance how we want to protect ourselves – we have a head start. By driving our protections closer to those assets – with tools like advanced identity, encryption, etc., - we raise the bar.

Now, to help me set-up my 4th tip…There is a little known American philosopher that recently provided a profound piece of insight…

Mike wanted to start every fight by hitting you so hard, you got scared. After that first punch, everything changed.

If you're a heavyweight prize fighter getting ready to fight Mike Tyson, you need to be training and sparring with someone as big, as strong, and as fast as Mike Tyson.

So NUMBER 4 - PRESSURE TEST SECURITY CAPABILITIES by engaging "white hat" external hackers to simulate attacks.

If you're going to defend against advanced adversaries, you need to test your program with the same veracity as the adversary – the same tactics, tools and procedures. The bad guys aren't using automated scanners to break into your enterprise during off peak hours, with "kid gloves" on… they're swinging like Mike Tyson with focused purpose.

This is the only way you'll know if you're ready to remain resilient.

NUMBER 5 - INVEST TO INNOVATE AND OUTMANEUVER, continually innovating to stay ahead of attackers.

We all have a lot to do – and that's in the face of shrinking budgets. The last think you're probably thinking about is innovation. It is challenging enough just keeping the boat afloat.

Based on our client experiences, one of the common traits of the highest security program performers is the wisdom to continually look ahead. Our adversaries are innovating constantly – testing code, creating zero-day exploits, pushing the boundaries. Your program should have an element of the same. Don't simply wait for vendors to innovate – push the limits of technology, try unconventional approaches, think out and around the box – stand on it, flip it over – try to break it yourself. It's a lot of fun for your team, and it will yield strong returns for your security program.

AND FINALLY, NUMBER 6 - GROW CONFIDENTLY by keeping security connected to the bottom line and to real business needs

At the end of the day, Cybersecurity isn't a technology problem, it's a business problem. And like all business challenges, we can't remove all of the risk – nor should we. Through the items we just discussed, we can make this a manageable and solvable problem.

So there you have it. The three things you need to understand to dramatically improve your cybersecurity performance and beat the bad guys:

1.) While we've made amazing progress, we still have a fair amount of room to grow,

2.) We need news way of thinking about the cybersecurity problem – because the way we're approaching it now isn't working,

3.) This is actually solvable when we break the problem into manageable chunks.

I hope that resonated for you.

It's going to be great letting this [Kevin: show the $5 gift card] simply mean I'm going to get a great cup of coffee.

Thank you for your time today.

[Kevin: Slight Pause]

We have a few questions that have been queuing up but please use the Q&A box to submit your own questions.

[Go Get iPad]

That's all the time we have for questions, but I encourage you to check out our research and stay connected via our social channels. You'll find links in the downloads area of the webcast platform.

A big thanks to our Accenture Alumni community for tuning in. Please be sure to complete a quick survey to help shape your next alumni webcast event. Have a great day.