accenture

THE PATH TO CYBER RESILIENCE

AUDIO TRANSCRIPT

0:00

MUS

SAMY: One day, you know, my mom was able to get a computer and bring it home, and this was the best day of my life.

ELISE: This is Samy Kamkar. And he's talking about the very first day he got online.

JOSH: For anyone… of a certain age… you may remember the glory of the early internet. Being able to connect with people all around the world right from your family's computer room. To Samy, it was magical.

SAMY: I got on the internet, I started searching… I found message boards, and I could like, talk to people… but I'd have to just sit there and wait and refresh and refresh.

ELISE: But Samy found very quickly that not everyone on the net was chatting away with pure intentions…

SAMY: I jumped in a room and said, "Hey, who wants to chat?" And someone said, "Get out."

MUS out

And I said, "Wait, what?" And 10 seconds later, the computer, the brand new computer that my mom just got crashes. I get this blue screen…

JOSH: The infamous blue screen of death. Samy had no idea what had just happened. One minute he was in a

1:00

chat room, and the next, it seemed like someone had reached through his computer and shut it down. He thought he AND his brand new computer were goners.

SAMY: And I freak out. I'm 10 years old, I'm gonna be grounded for the rest of my life.

ELISE: In a desperate attempt to fix it, Samy completely unplugged his computer. And then… he waited.

SAMY: I wait maybe half an hour… I plugged everything back in. I wait two minutes for everything to start up.

And fortunately everything is okay.

MUS

JOSH: Samy breathed a huge sigh of relief. Right after he finished giving thanks to the computer gods for saving him from certain grounding, he started to wonder… How did that anonymous person in the chat room shut down his computer from possibly hundreds of thousands of miles away?

SAMY: I was terrified, but I also thought that was the coolest thing ever. How do I do that?

SAMY: And that's really what got me interested in computers and hacking and really understanding how this stuff works.

Josh: So he started learning how to write code. By the time he was 19, he was a full-fledged software engineer.

MUS out

ELISE: Throughout the decade

2:00
that Samy spent learning to hack, the internet had grown up around him. Chat rooms weren't the big thing anymore; social networks were starting to pop up.

SAMY: All my friends at the time were on this website called Myspace.com. And I was like, okay, I'll check it out.

JOSH: You might remember Myspace. Your profile had your picture and information about you. And it was cool because you could also customize your page. You could make your favorite music auto-play, or create your own special animated background. And this got Samy's hacker-mind turning…

SAMY: I was like, well, can I do something cool with my profile that other people can't do?

ELISE: That simple question led nineteen-year-old Samy Kamkar to create a virus. And it would change the world of cybersecurity forever.

SAMY: I realized, you know, I had made a mistake.

SAMY: I had created a worm.

THEME in

SAMY: I didn't know even what it was called. I was just messing around on a social network. And apparently people never realize that this thing could proliferate so quickly.

[**Text Wrapping Break**]**SAMY**: And I think to this day it is still the fastest spreading virus in history.

3:00
ELISE: I'm Elise Hu.

JOSH: And I'm Josh Klein.

ELISE: And this is Built for Change, a podcast from Accenture.

ELISE: Samy's story is bringing me back to those early days of dial-up internet.

ELISE: What did getting online sound like for you, Josh?

JOSH: [Modem noise]

ELISE: [Laughs] Okay, for me it was more like… [Beeping internet connection noise]

JOSH: [Laughs]

ELISE: Oh, oh the memories.

ELISE: Obviously A LOT has changed since then, but cyber attacks have been around as long as the internet has. They're a fact of life online. And as tech evolves, cyber attacks do too.

JOSH: That's true. And the vulnerability and uncertainty of the pandemic really escalated this, right? You know, cyber attacks have really been on the rise. So now at this point it's not a matter of if your company's gonna be the victim of an attack, but rather when it DOES happen, whether you'll be able to bounce back stronger than before.

ELISE: Yep. So in this episode

4:00
we'll look at how businesses can align their core mission with their cybersecurity strategy to make sure they're ready for whatever cyber risks might come their way. But first, let's go back to see how Samy Worm changed the landscape of cybersecurity in the first place.

THEME OUT

MUS

ELISE: The year Samy created the virus was 2005. At that time on Myspace, users could easily modify their profiles, so each Myspace page was kind of… unique.

SAMY: People would just have extremely obnoxious … colors and blinking lights. There were categories like your favorite movies and books and heroes.

ELISE: So Samy could have easily created a page with a big, blinking marquee and neon green background that listed his favorite TV shows. But Samy's goal was to do something with his page that no one else could.

SAMY: I started playing around and reverse engineering. Like, can you see how it works? And of course I'm not trying to do anything malicious, I just think it's kind of funny.

ELISE: Pretty quickly, Samy found a gap in

5:00

Myspace's web security that let him edit the standardized elements on his Myspace profile. Like even though Myspace only allowed for 12 photos to display on your page at once, he made it so that his profile had 13 photos.

MUS out

SAMY: I was like, that's kinda neat. I just thought, what else could I do here that'd be interesting?

ELISE: Samy kept pushing the envelope. His next step was not just to change his profile… but to change OTHER people's profiles…

SAMY: So let's say they visit my profile. I can make them click add me as a friend. I can even make them modify their own profile.

ELISE: So now if a Myspace user visited Samy's profile, the virus would do two things. One, it would automatically send him a friend request. And two, it would add a brand new line of text to the user's profile page, that said….

SAMY: "But most of all, Samy's my hero"

SAMY: I thought, that's kind of funny, like a couple people will probably visit my profile over the next week. And at that point they'll see that and they'll laugh and maybe … myspace will remove it and whatever, no big deal.

MUS

ELISE: But a few days went

6:00
by… and nobody had visited Samy's page. His plan to add "But most of all, Samy's my hero" to a few unsuspecting people's profiles wasn't working.

SAMY: So I thought, okay, well, how do I make the spread a little faster?

ELISE: Samy adjusted the code so that it would copy itself. That meant that if you, an innocent Myspace user, visited a friend's profile that had originally been infected by visiting Samy's page, your profile would get infected too. Then anyone who visited your profile would also get infected.

SAMY: I put it on my profile one night and I went to sleep and I was hoping to get one or two friends by the morning.

ELISE: But when Samy woke up the next morning, he found something very different waiting for him on his Myspace page.

SAMY: And I check my profile and I have 10,000 new friends up from my 20. And I realized, oh no, I've, I've made a huge mistake.

ELISE: Samy had created a worm, a self-replicating virus. The Samy Worm. The infection moved swiftly from

7:00
computer to computer. Myspace was one of the most trafficked sites on the internet in 2005. But it was nowhere near prepared for this kind of fast-moving attack. Within less than 24 hours from launching, Samy saw the worm growing at a rapid rate—growing from 100,000 people to 500,000 people to a million people infected.

SAMY: I see about 3000 people per second, getting infected

SAMY: Finally they take my profile down. And I'm so glad.

ELISE: But Samy's relief didn't last long.

SAMY: And then … I saw the entire site is down. And I felt awful. I felt absolutely terrible.

ELISE: Myspace was completely shut down for about two hours. And when Samy finally managed to pull the site back up… he saw that his profile had been deleted.

MUS out

Meanwhile, Samy sat tight. For months he didn't hear a peep from Myspace, or see any consequences from setting the worm free.

But one day, as Samy was walking down from his apartment to his car, he got a sinking feeling in the pit of his stomach.

8:00

SAMY: I see two guys sitting on my car and I realize… I'm getting carjacked and I walk up and two more guys walk behind me. And I'm surrounded by four guys now. And they say, “Samy?” And I think about it. I realize carjackers don't know your name. And they say “Samy, we have a search warrant.”

ELISE: In the end, Samy was raided by the LA District Attorney, California Highway Patrol, the US Secret Service AND the Electronic Crimes Task Force. They took his computer, all his files.

SAMY: They said that they want me to never be able to touch the computer again, never touch the internet again.

MUS

ELISE: The Samy Worm itself caused some damage by shutting down Myspace's entire website. It also caused a fair bit of panic. Samy used a hacking technique called a “Cross-Site-Scripting” attack. It was the kind of virus that hackers could use to inject malicious code into a trusted website, exposing anyone who visited the site to having their data stolen, or worse.

Most cybersecurity experts at the time knew that websites were vulnerable to this kind of attack. But most

9:00

websites didn't realize just how much havoc it could cause, so they didn't bother to protect against it… until Samy came along and demonstrated how an attack like this could have an immediate, widespread effect.

Fortunately, Samy Worm was actually pretty benign for a cyberattack that affected a million people. It didn't target people's data. It wasn't malicious. It just made Samy everyone's hero.

MUS out

So Samy and the State of California came to a plea agreement. Samy had to pay restitution, go on probation, and was banned from using the Internet and computers.

SAMY: I didn't touch a computer or the internet for three or four years.

ELISE: After that, the charges were lifted and he became a normal citizen again.

But in all that time away from the internet, Samy started to think about hacking in a different way. The skills he'd built to become a great hacker could be used for good. To make systems stronger. More impervious to attacks.

SAMY: I still want to understand, I still want

10:00

to break things down, but I don't want to do it in a way that's malicious or really harming companies or people. So how can I do this in a way that is at least positive or interesting?

MUS

ELISE: Myspace had a gap in its web security. A gap that a lot of other companies also had at the time. In fact, in 2005, about 90% of websites were vulnerable to the attack that Samy carried out.

And following the attack, Myspace knew exactly where it had to patch things.

SAMY: I think it was the first demonstration of an attack that could impact many people very quickly. And that just hadn't been demonstrated before.

ELISE: The landscape of cyber attacks is different now, and that's partly because of Samy Worm.

SAMY: Understanding that you could really just weaponize this type of attack into doing something actually much, much worse. I think that was a big wake up call for companies to understand oh, we needed to actually take cybersecurity seriously, because there are attacks that are going to be more than just one person being hacked. It is possible to attack a million people overnight.

11:00

MUS out

JOSH: So I remember first hearing about the Samy Worm.

ELISE: Wow.

JOSH: You know I was really interested in cybersecurity and hacking and cracking, and a lot of my friends were, and then the next day… my grandma was asking about it, you know, like it was a huge shift in public consciousness.

ELISE: Huh!

JOSH: Yeah, companies suddenly realized it wasn't enough just to build cool software. You had to build cool software and defend it.

Elise: Yes. Threats have only gotten more sophisticated since then.

JOSH: Yeah. Now it's not a matter of if it's a matter of when.

ELISE: So next we'll learn exactly how companies can respond to the constantly changing cybersecurity landscape: how attacks take shape and what companies can do to stop them and recover from them. So they can learn from those lessons to come out stronger than before.

MUS

JACKY: The biggest thing that an organization wants to do is to continue its business in peace. So if that's disrupted, it's very serious.

ELISE: This is Jacky Fox. She's the European Lead for Security at Accenture. She's talking about how the everyday operations of a company

12:00

can be totally disrupted when a cyberattack happens.

JACKY: A cyber attack usually insinuates that it's something that's coming from outside and attacking your network. It also tends to have that cloak of anonymity around it as well, that you can't immediately identify what it is that's happening to your organization.

MUS out

ELISE: What makes a cyber attack particularly tricky is that it can take many forms.

MUS

It could be an attack on the availability of your system. Think of it like a big brick wall going up between you and all your operations. Like if a banking website got hacked, users wouldn't be able to log in to their accounts on the front end, and employees wouldn’t be able to log in on the backend either.

Or, there’s data theft - That targets your customers’ confidential information, like names, addresses, even personal identification numbers.

An attack could also be indirect, like hackers getting sensitive information about your company because of a breach at a different company that’s part of your supply chain.

13:00
MUS out

JACKY: This is no longer an IT and a technology problem. It’s about the survival of the business… That means … challenging the senior exec and the boards to say, how are you securing this organization? What would happen if we were hit? Would we survive?

ELISE: It’s an increasingly important question. The recent State of Cyber Resilience report by Accenture found that from 2020 to 2021 the average number of cyber attacks per company increased by 31%, to an average of 270 total cyber attacks.

That’s 270 attacks on a single company in just one year.

JACKY: When you've got a bigger, public facing area of your organization. Inherently, there are going to be more vulnerabilities there that people can attack.

ELISE: For example, consider the cloud. In the shift to remote work during the pandemic, a lot of businesses transitioned from “walled networks” in their offices to the cloud, which created a new digital space to secure.

JACKY: So you, yourself as an organization

14:00
don't necessarily need to be a target. You can't say, “Nobody's ever going to come near us because we're not significant,” because you could just be in the link or the chain, or sometimes just having a particular type of technology can put you in the firing line.

ELISE: Jacky says it’s not a matter of if you get attacked, but when.

JACKY: You have to accept that you’re going to be attacked.

MUS

ELISE: So let’s say an attack is inevitable. You certainly want to put up your best defense. Jacky says that prevention may be better—and certainly cheaper—than the cure. The cost of recovery can be thirty times the cost of prevention. There are the losses that can add up while companies are down, but costs also pile up from rebuilding systems, devices, networks, and paying people to do that.

So it’s worth investing in defense. But Jacky says businesses need to do so with the right priorities in mind.

JACKY: You could keep spending money forever on cybersecurity… If you don't strategically align it with your business objectives

15:00
and protect your real crown jewels and the things you really need to protect, you may as well be throwing money away.

MUS out

ELISE: So here’s the crux of it: The best defense comes from aligning your business and cybersecurity strategies. So, what does that mean?

JACKY: You can't afford to protect everything in exactly the same way. You need to focus on what your key assets are, whatever it is that is your raison d’etre. That's the thing that you need to focus your defenses around.

ELISE: Jacky says the first step is getting clear on your business's priorities. So for example, for a credit card company it would be really important to keep customer's personal information secure. That's core to the mission of the business, so the company would really want to invest in protecting that data.

MUS

The second step in aligning your business and cyber strategies is to get teams that might not normally work together all on the same page.

JACKY: It is so important that the business and the security teams talk to each other and understand what each other's needs are.

JACKY: Actually having a really good

16:00

relationship and a trust relationship between the two so that they can speak the same language.

ELISE: One time, Jacky was working with an organization that decided that if an attack happened, they'd just cut off all communication between their business and the internet. The idea was, if they turn the internet off, then the hackers won't be able to get in.

BUT the cyber team didn't mention their plan to another team inside the organization, responsible for business resilience.

JACKY: They also had a business resilience strategy that if one internet service provider got cut off, that another one would pop up [laughter] as part of their business continuity.

ELISE: It was like cybersecurity whack-a-mole. But the business was playing both the whacker and the mole.

JACKY: They shut this down, and then, "Bing!", it popped up over there, you know? So if that happened in a real attack, and you thought you were cutting off an attacker and you weren't at all, like, things like that are so important.

MUS out

ELISE: Jacky says that in order for a business to fully align their cybersecurity and business strategies, the CISO needs to be fully involved.

MUS

17:00

The CISO, is the Chief Information Security Officer. So say, a business is launching a new product…

JACKY: So the CISO says, well, you know what, while you're designing that new product it's really important that you architect in these specific controls because that's going to protect us.

And all the way through while the product's being made and designed, they're checking in with the team, they're getting it tested… You know as the product design changes because something happened and it didn't work, they run it by the security team again. So they're working together all the way while that product is being produced.

So when it comes to the couple of weeks before it goes to market, and they're doing that final independent testing on it, the likelihood is that they're going to pass with really good colors going through.

MUS out

ELISE: But attacks do happen. What matters after an attack is how you recover. Which brings us to cyber resilience, the real test of a company's ability to respond quickly to threats, minimize damage and continue to operate while under attack.

18:00

MUS

JACKY: Cyber resilience is your ability to recover post-attack. You know, it's like a flu, how long does it take you to get over that flu? That's how resilient you are to the virus. And it's not that dissimilar in the cyber world. You get attacked. How resilient will you be to that? How quickly will you recover? What kind of losses are you going to have financially?

ELISE: The Accenture State of Cyber Resilience report surveyed companies across 23 industries in 18 countries, and evaluated their Cyber Resilience. And the results were pretty surprising. At the bottom of the ranking is what Accenture calls Cyber Vulnerable organizations.

This is 55 percent of companies surveyed.

JACKY: Their security is neither aligned with their business strategy nor is it very resilient. If you're in that group of the vulnerable and you get hit, the chances of your organization surviving are quite slim.

ELISE: And that's not hyperbole. Jacky's done the math.

JACKY: If you have enough funding to keep

19:00

salaries being paid, keep the lights on, do whatever it is you need to do for 30 days. And you can't recover your systems within 30 days, then your organization goes out of business. So that mean time to recovery, if it's bigger than your financial ability to survive, you can get into real trouble.

ELISE: Then, moving up the ladder, Jacky says there are Business Blockers and Cyber Risk Takers, who only prioritize either cyber resiliency or business growth, but never both in alignment. And then, there are those who are the leaders of the pack. Only 5% of companies. They're called Cyber Champions.

JACKY: They're the ones that we see they have a good balance between how resilient they are as an organization and also meeting their business objectives. They are applying their cyber controls and their cyber budget into the right areas, which allows them to recover faster and spot more things before they become a real issue for them.

ELISE: Cyber Champions fold security into their business priorities - so they're better

20:00

at stopping attacks, finding and fixing breaches faster and reducing their impact.

MUS out

Because, of course, even Cyber Champions get hacked. Remember, it's when - not if.

MUS

Jacky says for any business suffering an attack, the first thing to know is that there is no shame in being a victim.

JACKY: I would say, five to 10 years ago when people got attacked, they didn't want anybody to know about it.

ELISE: Really, no companies like to talk about their hacks. But Jacky says, that's changing.

JACKY: I think the culture has shifted a little bit away from the blame game, and actually, a culture of sharing the learnings from that and the intelligence that you've gleaned from that is going to help other organizations.

ELISE: To recover your systems quickly and survive, having learned valuable lessons that made your business stronger? That's the hallmark of a Cyber Champion.

JACKY: You know, nobody is going to be perfect every day.

JACKY: I really admire organizations that come out and do a lessons learned and publish no matter how embarrassing it is.

21:00
Cause it's just the right thing to do.

MUS out

JOSH: I love how Jacky brings up that sharing attacks that companies have experienced is so critical because for a long time companies, if they got hacked, they wouldn't share it.

ELISE: Yeah, they felt ashamed, right?

JOSH Yeah. No one could grow or improve. You couldn't learn to defend against it cause you didn't know it existed.

ELISE: Yeah, yeah. And her example there of one hand not talking to the other too, another opportunity for learning.

JOSH: Absolutely. I mean, the truth is there's no one size fits all cybersecurity solution.

ELISE: Yup. The real necessity is making sure the teams are talking to each other and having cybersecurity knowledge baked into your product is even better. So next we'll look at how a certain hacker used his security expertise to strengthen his company and its cyber defense.

MUS

SAMY: If you want to be able to secure a system, you need to understand how it works. You need to understand how to break in.

ELISE: This is Samy Kamkar again.

SAMY: I'm really interested in how can I do this stuff in a way that actually helps people. Like how can you take a system that you have

22:00
and maybe take advantage of it in a beneficial way.

ELISE: The internet has come a long way since Samy Worm wreaked havoc on Myspace. And Samy's come a long way too. Now he uses this kind of thinking to create security solutions for his own business, Openpath.

SAMY: Openpath is a mobile and cloud based physical access control system. And it just means that you can walk into your business with your phone in your pocket and wave your hand to our reader. And that'll unlock the door.

ELISE: So, as long as you have your phone on you and you're in their database, with Openpath's readers, you can walk right into private places that would normally require a lock and key, or key card swipe.

MUS out

The technology works for offices, homes, garages, gates…

SAMY: It's really easy, really convenient, and we try to make it very secure as well.

MUS

ELISE: Samy is the company's co-founder and Chief Security Officer. So cyber defense is in the DNA of the business as well as the product.

SAMY: We … spent a lot of time designing and debating and challenging each other

23:00

internally to see, okay, well, how we thought we designed a system and now let's try to break it.

ELISE: The security solution is multilayered. On one level, security is physical, with the latest chips in Openpath's Smart Readers.

On the digital level, they have a firewalled database where a user's private information is stored; they use multifactor authentication and one-time passwords; and their cloud-based software automatically updates, keeping it secure from threats.

SAMY: There is no one thing you can do to be super secure so we can only do multiple things. So that if something fails, we know that there are fail safes.

ELISE: This dedication to security, how it's baked into the business, is what makes Openpath what Jacky would call a Cyber Champion.

MUS out

But even with Samy at the helm of security, the alignment between Openpath's business strategy and their security approach didn't just happen overnight. It took prioritization, investment, and most importantly, internal communication.

MUS

SAMY: We for example, would have internal phishing campaigns. So we would

24:00

attempt to see if we could get our own employees to enter some information and if they did, that's okay. We're doing this as a method of training. And we show them, here are the things that you can look out for. So when you do get these types of real attacks, you'll be able to say, oh, I should probably be cognizant of this or cautious.

ELISE: It was important to make sure everyone at Openpath was up to speed with cybersecurity because, although it sounds counterintuitive…

SAMY: Making something secure, generally throws in roadblocks. It often will make something more difficult to use and more challenging to use.

ELISE: Employees having to complete two-factor authentication in order to log into a system? Yeah, it can add an extra step in the process. And it can make systems more complex to use. Ultimately because the risks you're protecting the company from are themselves complex.

SAMY: You might have a hundred vulnerabilities when the system is first prototyped or designed and you need to solve all of them. And maybe you solve 99. But as an attacker, I only need to find one issue to get in.

MUS out

25:00

ELISE: Openpath dealt with a security threat shortly after their product launch, where they found a vulnerability within one of the chips in their Smart Readers. But because they had multiple layers of encryption, and didn't depend on the security of the chip, there were no vulnerabilities in their own system. That prevented hackers from being able to get any info from the Smart Readers. Openpath was able to continue business as usual.

SAMY: It didn't impact us at all. We didn't have to change anything. But it does just make us think more about, well, when we're designing new products. Okay. How do we ensure that we can try to prevent these types of attacks and what could happen next?

ELISE: Samy says he understands that a lot of companies have a difficult time investing in protection against a bogeyman they can't see. But it's crucial not to wait.

THEME IN

SAMY: This will help you in the future, even if you don't immediately see it. And I only know that because I've experienced it. If you believe you're going to have a long term business, that's going to be around for more than a year, people are going to attack.

So this will, help you. This will help your customers

26:00

continue to have faith in your product and your service and your capability to protect their information and whatever you've created that is valuable to you.

JOSH: The Openpath story is such a great example of how the business and the cyber strategies can be aligned and how that can really benefit a company.

ELISE: Yeah, yeah. And it kind of has to, I mean, their whole product is about security for consumers, too.

JOSH: That’s true, that’s true. They acknowledged that cyber attacks are going to happen and therefore they were able to focus on learning from them. I think all businesses should focus on that and sharing their lessons.

ELISE: Yes. Next time I see a high-profile company experience some sort of cyber attack, I know that I’ll have a lot more empathy and curiosity about it.

JOSH: Absolutely.

JOSH: To learn more about the trends in today’s episode, check out the State of Cybersecurity Resilience report at Accenture dot com slash Built For Change. It talks about the path to cyber resilience and what your business can do to become a Cyber Champion.

ELISE: Big thanks to Accenture’s Jacky Fox.

JOSH: And to Samy Kamkar for talking to us.

ELISE: Built For Change is a podcast from Accenture.

27:00

JOSH: More episodes are coming soon. Follow, subscribe, and if you like what you hear, leave us a review.

MUSIC OUT
27:13