Avast Business

White paper

Best Practices for Today's SMBs and MSPs

A CISO's Guide on Cybersecurity Solutions

16 September 2021

Avast Business

About the author

Rob Krug, Senior Security Architect, Avast Business

Rob has been in the network engineering and security space for over 30 years. His background includes extensive work with telecommunications, network design and management, and most importantly, network security. Specializing in security vulnerabilities, Rob has extensive experience in cryptography, ethical hacking, and reverse engineering of malware. Rob served in the U.S. Navy and also worked as a Data Security Analyst and Director of Engineering for multiple international service providers and vendors. Rob has designed, implemented, and maintained some of the most complex and secure networks imaginable.

Introduction

Avast CISO, Jaya Baloo, Discusses Cybersecurity Solutions for Today's SMBs

One size doesn't fit all when it comes to SMBs. Some may have a full IT team on staff. Others may not, and many are limited by resources and budget. With cyberattacks targeting SMBs at an all-time high, it's critical for MSPs to be having those conversations with SMBs about enterprise grade security protection, tailored exactly to their needs.

In an interview with Richard Tubb, the IT Business Growth Expert, Jaya Baloo covers:

- The best ways to present cybersecurity to SMBs and explain its importance
- The biggest cyber threats faced by SMBs today and the best defense strategy
- How SMBs with limited budgets and/or IT resources can still stay protected
- The importance of a response plan in case an SMB is impacted by a cyber attack

Contents

Avast Business

Jaya Baloo

Jaya is the Chief Security Information Officer at Avast, where she is responsible for information and data security, and overseeing cybersecurity. She has been working in the field of information security for 20 years with a focus on secure network architecture. She is a faculty member of Singularity University and also sits on a number of infosecurity boards. She has spoken widely at high-profile conferences such as RSA, TEDx, and Codemotion on topics including Lawful Interception, VoIP & Mobile Security, Cryptography, and Quantum Communications networks.

The role of a CISO

Richard Tubb: For people who may be unfamiliar with the term Chief Information Security Officer (CISO), how would you explain what a CISO is?

Jaya Baloo: A CISO is basically the place where the buck stops in terms of security. They provide the security and mission for the organization, and the plan going forward in terms of having a good understanding of the risks the organization is facing, and how to stop those risks from manifesting.

SMBs, cybersecurity, and the role of MSPs

Richard Tubb: Many MSPs, IT solution providers, and SMBs may not have the budget to have a CISO in place – for a CISO-less MSP or SMB, how would an MSP explain the need for cybersecurity to a small business?

Jaya Baloo: Fundamentally, the need for cybersecurity is the same for any business. You just need to make sure that you can keep doing business at the end of the day, and if cybersecurity poses a threat to the continuity of doing business, then you need to handle it effectively. It's different for a security company, where the core security IS your business. I always used to think it made things easier, but actually that's not the case. Pretty much all companies need to do the same thing. They need to understand where their biggest headaches are coming from. They need to pinpoint those headaches on their network systems and data, and then they need to be able to act on them when they occur. And that's basically it. If we can get those three things right, that's just as valid for a multinational firm as it is for a bakery.

> “
>
> Businesses need to understand where their biggest headaches are coming from. They need to pinpoint those headaches on their network systems and data, and then they need to be able to act in them when they occurs.

Richard Tubb: There's been a shift over the past few years. Cybersecurity previously was considered something that only enterprise companies had to worry about, but small businesses felt they as though they were immune. However, that's changed though, hasn't it? Nowadays, any company is considered a target by cyber criminals.

Jaya Baloo: I think that's actually been the case for a really long time. If you take a look at the data breaches, it tends to be the companies that think, "It'll happen somewhere else but not to me. They aren't interested in my data, they aren't targeting me," but I think what we tend to forget is that there aren't just targeted attackers out there. There are also very opportunistic attackers who don't really care who they hit, as long as they hit someone. And you see this kind of prevalence happening, specifically in areas like ransomware, where huge portions of the population are very ill-equipped to handle an attack. And when they do get hit, because of their lack of preparedness to handle the situation, they are completely victimized and often wind up paying the ransom. I think that's actually the saddest situation, that they feel so desperate to regain that business continuity and return to "business as usual." They just go ahead and pay the bad guys, without any guarantees that they'll ever get their data back.

Richard Tubb: How frustrating do you find that, when you see that happening in the world?

Jaya Baloo: It's hurting the weakest in our population. I feel the same way about these types of events as any other vulnerable population being attacked - whether it's animals or people who can't fend for themselves. I feel like we have a responsibility as a planet to help them, and not just the companies that are capable of doing it for themselves. I feel we have a responsibility to protect each other in this society that we've created.

Richard Tubb: Going back to small businesses, the press highlights a lot of security challenges that they're facing nowadays, and more and more people are realizing this can happen to anyone. This isn't just happening in the realm of enterprises and large businesses, cybercriminals are targeting anybody. For MSPs trying to educate small businesses that don't feel it will happen to them, how would you advise them to get the message across to those small businesses that everyone is a target?

Jaya Baloo: I'm really big on evidence-based material. don't believe that fear, uncertainty, and doubt is the way to get the message across. Just look at the facts. If it's an individual or opportunistic hackers who are hacking for fun, or cyber criminals who are hacking from a profit perspective, they really don't care who they hit. Look at the facts. Malware usually gets labeled as being highly focused and targeted on very specific entities. Actually, that's

"

Businesses need to I feel we have a responsibility to protect each other in this society that we've created.

not the case. If you take a look at Regin, the malware that was used to infect a very large telecommunications operator, it supposedly originated from the NSA and GCHQ working together to target this operator. What you'll actually see is that the verified infections actually targeted a whole bunch of small-medium enterprises and private individuals in that space. There is clear evidence that small businesses need to be concerned about state-sponsored attacks. They can be caught in the crossfire as collateral damage that ensues, because we are all so interconnected with each other.

> “I’m a proponent of having a good security practice, as a level of maturity that is part of your whole corporate responsibility.

MSPs and security effectiveness

Richard Tubb: You’ve said you’re a big fan of using metrics and statistics to get this message across rather than fear, uncertainty, and doubt. What metrics or KPIs would you suggest that MSPs use to measure security effectiveness? What KPIs should an MSP focus on?

Jaya Baloo: I don’t see the difference here being very drastic. What you need to think about is that when you get bigger as a company, you tend to do more of everything. It doesn’t necessarily mean you add a bigger degree of diversity, but you add a larger degree of depth to the things you are covering. For me, here’s the single metric: if we’d do one thing that would signify the actual maturity of ANY organization, big or small, it would be the average time to respond to vulnerabilities and incidents. And that’s it. I’ve been saying that from when I was working at KPN, when I was working with Verizon, and I’m saying it here as well. If we measure one metric, to signify maturity, it’s those days in between, because that is the opportune time for a hacker to get in and do all kinds of damage. If we have known vulnerabilities that are uncovered by a vulnerability scanner (and there are free ones out there, as well as the services you pay for, that will scan both your outside perimeter as well as the inside of your network for vulnerabilities), once we know about a weakness, how long does it take our organizations to step up and fix the vulnerability? That time in between, that open and close moment, that says everything about how ready you are to cope with new issues as they come along, specifically as far as the severity of those incidents is concerned, and that closure time. So if we see, for example, the latest Microsoft Patch Tuesday, and we take a look at the types of high critical remote code execution vulnerabilities, if we don’t get them closed within 24 or 48 hours, it tells you everything you need to know about the preparedness of an organization.

Richard Tubb: Do you think this could be used as a sales tool and an opportunity for MSPs to say, “Hey, here’s our effective closure time to these threats.” Could this be a metric in the industry to say who’s doing this well and who isn’t?

Jaya Baloo: While I'm not so fond of it being a sales tactic, what I am genuinely a fan of is having this mature understanding that we're never going to prevent vulnerabilities from happening. If you take a look at some of the code that's out there, we have millions and millions of lines of code, it's nearly impossible to weed out all of the bugs - ones that are either accidentally or intentionally placed. So the smartest way to deal with it is to say, "Hey, we know it's going to happen, we know stuff is going to go wrong, but we're going to be able to roll with the punches better, faster, and smarter than the attacker," and I think that's really all anyone can do. So rather than using it as a sales incentive, which again, might get you to only fix the stuff on the outside and not on the inside, I'm a proponent of having a good security practice, as a level of maturity that is part of your whole corporate responsibility.

Current trends in cybersecurity threats

Richard Tubb: You're working with small businesses and with MSPs, across the world, every single day on cybersecurity threats. What are the top cybersecurity threats that you're seeing emerging that SMBs are facing today?

Jaya Baloo: I really think the biggest problem is that SMBs don't have a lot of budget and resources. Most don't really have someone on staff who's only looking at security, so as a result, they tend to be not lacking, necessarily, in their defense, but just slower to react, or not having all of the preparedness enabled. No one is going to be a victim of ransomware if they have online and offline backups and they're disciplined about it. The companies that don't consider this part of their core business practices are the ones we need to worry about. I think that the biggest threats that we see are the ones that take advantage of a lack of resources and a lack of planning, such as: ransomware, phishing attempts (which are still very successful), supply chain attacks, and the ability to keep on top of all of the things that are regularly going wrong. Other threats occur where there are patches. The SMB just needs catch-up time, but that catch-up time also leaves them vulnerable. For example, if you saw the Citrix breach recently, what you saw was that by the time the patch was available, there were already active exploits. So an SMB might not be agile or quick enough to have known that, and even when they applied the patch, they'd need to have the ability to do forensics as well, which is what would've been required if using Citrix.

No CISO, no problem – security "must-haves" for SMBs

Richard Tubb: You've mentioned how many SMBs are limited by budget and IT resources. What would you say is the best cyber defense strategy that MSPs can recommend to their SMBs that perhaps don't have the budget to help keep them safe? What are the absolute essentials you'd recommend that SMBs should be adopting nowadays?

Jaya Baloo: You know, there's this great quote from *Sun Tzu: Try to handle problems when they are small.* I think that this is something an SMB can absolutely do. It is difficult for large companies to be quick, agile, and roll with certain things, but an SMB can take advantage of the lack of bureaucracy and leverage the strength of being small. They can think about how to plan ahead,

before there is an actual crisis. For example, they can plan ahead by having those backups, or having an antivirus, or having some form of network monitoring, and a basic defense. They can also have a really simple automated patching regime. These are small steps. Baby steps. If they plan ahead of the actual incident, there won't have to be crisis management later.

Cybersecurity compliance

Richard Tubb: So we've talked about cybersecurity. One of the things that I think has encouraged greater awareness of cybersecurity is compliance. In Europe, we have GDP and all around the world there are regional compliance rules, which are forcing businesses to take cybersecurity seriously. How would you recommend that an SMB stays on top of these varying compliance routines?

Jaya Baloo: In general, I believe compliance is the floor and not the ceiling. So, compliance is the bare minimum of things you need to do. It doesn't ensure any form of security, and for an SMB, I would say that if you aim for security, you'll hit compliance every time. The focus should be on security and privacy. There will be compliance and regulation that keep coming, but that is not the place to keep your eyeball. Keep the focus on that ceiling of good security and good privacy practice. That's where we should aim. If we look there, we'll land there, instead of just doing the compliance minimum. Compliance has to be something that everyone can adopt, and everyone can manage. Consider the smartest things we can do, how we can plan ahead, and how we can think about smart partnerships to ensure our supply chains are doing the same things that we are. Those are things that I think an SMB can do to be powerful and act on, again, using their size and their ability to leverage those smart partnerships and their budget. They need to do it right, in the beginning, without waiting for compliance to hit.

Compliance is the bare minimum, and striving for more should be every business' approach.

Being prepared in case of a cyber attack

Richard Tubb: In the event that an SMB does experience a cybersecurity attack, what would your recommendation be for a response?

Jaya Baloo: IPlan ahead. While you can't plan for everything, you must have a plan in place in case something bad does happen. Otherwise, how are we going to figure out what's happened? It's not just SMBs, it's every company. They want to jump over that incident as quickly as possible and get back to business as usual, forget that it never happened, and push it way behind them. Never waste a good incident when it does happen, that's a rule of thumb. Hopefully, if it happens, you're not going to wipe all the data from the incident that tells you what on earth went wrong, because then you actually destroy your own ability to learn from that event and move on. Also, to understand the scope or the extent of damage, it becomes really important to preserve that forensic material and that evidence. Here are three things I recommend:

- Get a plan. Understand what you will do and what things you can foresee. You can't foresee it all.

- Have a backup strategy or a partner that you can work with. One of the options there is to work with a forensic company on retainer, so if something happens, you've got a company who can immediately help you on-site and help you get back to business as usual. This is why planning ahead is so important. You don't want all these unexpected costs, so know what that cost is going to be, and know if they are going to try to extort you at the moment of the actual incident.
- Have a deep knowledge about all of those super vital assets, so for the duration of the incident, you can still continue to do business. Whether that means understanding that the vital asset was compromised and having a backup, or having a disaster recovery plan even if it's on paper or on a spreadsheet, that's a great thing. Many large companies don't have it, so again, take advantage of the small size to think intelligently about this. If you can't be bigger, you have to be smarter.

> "While you can't plan for everything, you must have a plan in place in case something bad does happen.

Richard Tubb: Are there any online resources you would recommend that SMBs can check out to help put together this response plan?

Jaya Baloo: I try to open source everything that I've ever worked on in my career. When I was at KPN, we open sourced our security policy, so it was always out there. I would say copy with pride! There is no shame in taking good lessons from others, and if you just Google 'simple disaster recovery plans,' you'll find them. All of this stuff is findable, thanks to Google, and thanks to that open community of security people online.

The role of the SMB staff

Richard Tubb: Let's talk about the role that SMB staff play. And specifically, how MSPs can educate those staff members. We both know that the weakest link in any security chain is a human being, and there is no accounting for that. How can SMBs raise cybersecurity awareness amongst their employees?

Jaya Baloo: I think we tend to forget that we are multi-faceted. We are employees but we're also humans, with our own private sphere of things we do, and things we do online as well. A really simple thing is to have them understand security for themselves. It's one thing when the motivation to understand security is coming from an employer, but it's quite something else when you talk about the motivation of being secure for the individual, not the employee. When it's about the individual, it's about being safe online from your family perspective, from your home perspective, from your own online banking situation, and your own personal credentials. So I would encourage users, for example, to take their private email addresses and use the free service haveibeenpwned.com. Set up an alert for your own email address and just see if it's ever been previously compromised in any data breach for any of

the brands you trust. All of us have been there, because there have been so many data breaches. So it's highly unlikely that you have no addresses in the last X amount of years that haven't been found on one of those sites on haveibeenpwned.com. That's usually a wake-up call for people who have no understanding of security. And from a corporate perspective, from an employee perspective, you could subscribe to a service like SpyCloud. There are so many services where you can enter your corporate email addresses and see if they've been compromised in a potential data breach.

Again, I urge caution to not create fear, uncertainty, or doubt. You want people to be able to enjoy technology and all of its benefits without worrying about their security and privacy. They just need to understand the trade-off.

Emerging technologies and the future cybersecurity landscape

Richard Tubb: We've talked about the present state of cybersecurity and that there's some scary stuff out there – but it can be managed. What does the future cybersecurity landscape look like? What emerging technologies do you expect will play a major role in cybersecurity defense?

Jaya Baloo: There's a lot of hype and buzz around all things AI, but I have to separate the fear here. There are always questions like, "Will the attackers use artificial intelligence to launch super attacks that we can't defend against?" The honest answer is no. No one has seen an AI-delivered attack. The only place you see it is with machine learning and domain generating algorithms where they are continually used. But as far as AI attacks against our defenses is concerned, this has yet to be spotted. This is simple for the defenders in the sense that we have a timeframe, where the advantage is in the hands of the defenders to defend. But that advantage is short lived. The moment we don't capitalize on that advantage and shore up all of our defenses globally, the easier we make it for the attackers to obtain that same technology and use it in order to strike. At that point, the cost of using AI techniques will inevitably decrease, and we'll be too late. So, I really believe that we need to start figuring out how to use AI for anomaly detection (that is, identifying abnormal behavior within a dataset). We need to start consolidating all of our data (information that's often housed in logs in different places), and use AI to identify trends to better anticipate attacks.

There's a matrix you may have seen for defenders from Mitre called the Mitre ATT&CK framework. It basically shows you the lifecycle of an attack and how it would occur. It's a wonderful framework to use and for a defender to understand. It shows how the attacker moves through the stages of attack to an eventual compromise. By utilizing tools like the Mitre ATT&CK framework and AI for anomaly detection, we'll be able to learn how to better anticipate cyber attacks based on the large volumes of historical data that we have, and act quicker. Truly understanding how an attack occurred from beginning to end, as well as the different components involved, will help us to be more prepared in the future

Avast Business

Jaya's take on cybersecurity

Richard Tubb: We talked about the implications of cybersecurity and how scary it can be for SMBs. You're working with the biggest companies in the world. You're seeing exploits as they happen, in real time. Do you get scared about cybersecurity? What excites you about the role that you are in? What excites you about cybersecurity?

Jaya Baloo: I'll start with the first question. Do I get scared? The thing that makes me most afraid is our inability as humans to adapt to change. We are terrible at adopting new standards. We are slow. We are unwilling to face facts or evidence. We are far more likely to jump at hype, to jump at fear. Those are the things that move us, and it's really unfortunate because I feel like these are the wrong incentives, the wrong reasons to move. But you know, this is invariably what works among our population and although that's the case, it makes the face of this cybersecurity landscape incredibly dynamic. It means it is fast moving. And the thing that excites me most is that the companies I've worked for allow us to have a true and meaningful impact, to protect the weakest among our population.

MSPs: attracting the right talent

Richard Tubb: For any MSPs saying, "We want someone like Jaya working for us," how can they attract people of your mindset, to work within their business?

Jaya Baloo: I think first and foremost it should be a meritocracy. It should be people who deserve to be where they are, who are like minded spirits. And that's another thing. Within the security community, there are a lot of people who know each other, and they cross-network and cross-recommend each other. So I think looking at and approaching the community like, "Hey, who do you know?" is the way to do it. If you're completely out of that community, go online, go to Twitter, go to Google, go to LinkedIn, these are all great resources and all great places to find like-minded individuals. There are so many good people out there, and it always amazes me that we don't know how to find, attract, and encourage them the way that we should. This is also just about outreach from us. If we're going to be very traditional and very closed, we're never going to get those people who are the opposite, so we really just need to extend that hand.

To discuss any of these topics, or for any other related questions, you can reach Jaya on Twitter at @jayabaloo.

About Avast Business

Avast Business provides integrated, enterprise-grade endpoint and network security solutions for SMBs and IT service providers Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. The result is superior protection that businesses can count on. For more information about our managed services and cybersecurity solutions, visit **www.avast.com/business**.