Commercial Insights with Regions Bank

Episode #18
How to Manage Cybersecurity Risk
Global cybersecurity spending is set to exceed $1.25 trillion by 2025 — but how and why is spending changing? Companies need to know where the risks are now, plus how to find the internal and external people, processes, and technology to mitigate those risks. In this episode, get insight for planning budgets and risk management strategies to fight cyber threats.

Episode Transcript
Chris Smoak, SVP, Head of IT & Data Risk Management

It's important to establish what we call a risk appetite. And that speaks to the amount and type of risk that your organization is willing to carry. This really allows you to balance investment, to align with that appetite, to ensure you're investing appropriately, but critically not overinvesting in certain areas where there might be less of a return on investment.

Chris Blose, Host:
Welcome to Commercial Insights with Regions Bank. I'm your host, Chris Blose, and you've just heard from Chris Smoak, senior vice president in charge of technology, cybersecurity and data risk management.

When Smoak mentions risk appetite, he's talking specifically about cybersecurity, the topic of today's podcast — and the subject of many a shocking headline. When a company gets attacked, when private data becomes public because of a breach, or when risk leads to losses, the public often hears about it. And it's a threat to a company's operations and bottom line.

Today, Smoak is here to offer perspective on what businesses in 2022 need to know about cybersecurity, and the steps they can take to protect themselves.

Chris Blose:
Let's put things into context to start. When a company looks at its biggest risks in 2022, what are they?

Chris Smoak:
The risks have always been there, right. The real challenge, I think, is that the attacks are much more prevalent today. We see that in many incidents that we've seen reported in the greater news media. And whether it's your customers, or employees, or maybe even your applications, they all have vulnerabilities that can be exploited to drive an impact in the organization.

So Chris, I think, in my mind, one of the biggest challenges is really understanding the importance — both the technical, the bits and the bytes. But also the business perspective that we're talking about here in cybersecurity. In other words, what does a cyber attack mean to an organization's ability to conduct business? You know, what does it mean for a potential monetary loss?

Chris Blose:
You mentioned the technical aspects of cybersecurity. Is that daunting for people? And how do you put the threats into practical terms for them?

Chris Smoak:
I think it really comes down to separating yourself from those bits and bytes we talked about, and really driving what it means to an organization. So, instead of saying, "You have a particular vulnerability on a web application," you know, understanding the web application itself, what type of data it houses, what type of business process it works for the organization, then how the loss of that or how the exposure of some of that data might impact the business in terms of, you know, privacy concerns, compliance concerns, as well as general downtime and unavailability of the systems to those customers.

Chris Blose:
So how do you advise people to look for red flags to avoid those impacts?

Chris Smoak:
So I always talk about a balance between three things, Chris: people, process and technology. Any, you know, large gaps between any of those can be a red flag for you to take note within your own organization. So when I speak to business leaders, it's really focused on assessing the maturity of each of those three areas and seeing if maybe you're ahead on a couple, but maybe behind on another.

For example, ensuring your organization has the proper policies, procedures and standards in place to establish that baseline expectation is really key. You'll need to have things like incident response plans, procedures, remaining vulnerabilities and patching, and test that those work as expected. And then you couple that with strong people to help manage and refine those processes. Also, Chris, I'd say equip those people with tools to empower and enhance the work that they do.

It's important, I think, to establish what we call a risk appetite. And that speaks to the amount and type of risk that your organization is willing to carry. This really allows you to balance investment, to align with that appetite, to ensure you're investing appropriately, but critically not over investing in certain areas where there might be less of a return on investment.

Chris Blose:
So balance sounds key. What questions can an organization ask to get to that balanced investment?

Chris Smoak:
The best way to think about this is to start at the high level. You know, look at what type of resources are out there to help organizations identify and fill in those gaps. So, for example, a quick search on the web will give you a number of very reputable sources for cybersecurity frameworks. But I think one popular option to look for is the National Institute for Standards and Technology. They have a cybersecurity framework published on their website that really helps you understand what threats are, what vulnerabilities are, and what those impacts could be. And critically, they help you understand mitigation options for each.

And in addition, I'd say depending on your industry, there may be more specific information, or perhaps groups that are available to help you inform the roadmap and in more of a specific way that's aligned to your business.

Chris Blose:
Now on the process side of the people, processes and technology triangle, is that usually a matter of up-front strategy or after-the-fact response? Or perhaps a bit of both?

Chris Smoak:
I think it's really a combination of both. I mean, the key thing here is to take some time ahead of time, before you have a cybersecurity incident, to understand what you'd like to do. If and when we see a particular exploit or vulnerability in our applications, or when we see malicious software in our environment, what do we do? Understanding that and being able to go through that process in a way that's methodical, without some of the emotional concerns of responding to an incident in the wild, is really important.

I think that's the real key. A lot of us, we get very worried when we think about cyber risk. If you or anyone has been impacted by it in the past, it's not a great thing to go through. We understand that the frame of mind someone would go through when you're responding to an event, it just needs to be second nature for you, what you wanna do, how you wanna do it. And this process really helps you establish that and feel comfortable so you can rationally work through a process.

Chris Blose:
I assume some of that focus is so you don’t take a reputational hit with a bad response, right?

Chris Smoak:
Absolutely. Customers, investors, regulatory entities want to understand what happened to an organization when they announce a breach. And there's an emphasis on trying to do that quickly. The challenging part here, Chris, when you think about how you respond to an incident, especially a large cybersecurity incident is, it takes quite a lot of time to understand the full depth and breadth of an attack. What happened, was any data accessed, if so, how much?

Being able to work through that process and articulate it to external parties can really help give confidence that you're doing the right thing, and you're doing it in a way that's repeatable, that they can understand and see.

Chris Blose:
You brought up risk appetite. So with everything that’s changed in the past couple of years, how has that risk appetite — or even specific threats — changed, too?

Chris Smoak:
There's certainly been a lot of concern with the shift to remote and hybrid work over the past two years. While there's really been increased concern of the internal fraud piece of it, the external cyber risk environment remains relatively consistent, which is a little bit unique for us. The focus for many organizations really is ensuring that employees have the right access to the resources they need to do their job. And we haven't really seen a tremendous impact specifically on the cybersecurity risk in that area. But what it does mean is that a business will really face different legal constraints based on operating in different states or countries, and as well as particularly privacy laws we've seen come about over the last few years.

Chris Smoak:
I think I'd be remiss if I didn't mention ransomware here, though. We've, we've all heard of it, unfortunately, over the last couple of years. And while the concept of ransomware has been around for many, many years, we've seen a dramatic uptick in the impact and the visibility more recently.

You know, as a real quick refresher, ransomware is a malicious software that encrypts data on your business's computers and systems, which effectively makes it impossible to access. More recently, we've seen instances as well where attackers have also stolen that data in addition to making it unavailable. And the attackers then really attempt to trade some form of monetary payment.

You know, many organizations struggle with paying the ransom in hopes of getting back into operation more quickly, or trying to recover themselves, which, as you might imagine, can be a real big challenge. That generally takes longer, but it also doesn't necessarily incentivize attackers to come back.

While ransomware is unique in a few ways, I think one thing to keep in mind is that it's not all that different from other cyber security related threats that we face. And so we talk about having a strong security program, including detection and response. All that can help really prevent ransomware from taking the original foothold in your organization and making a challenge to mitigate.

One other item I'd mentioned here, Chris, is how a lot of what I'm speaking about today really applies not just to your organization, your business. It also applies to the vendors and partners you work with. In recent years, we've seen a dramatic uptick in attacks against third parties, where the overall target is your business, but it might come through one, (laughs), of your suppliers or third parties.

Chris Blose:
I think those upstream threats are on a lot of people's minds more now than they were in the past, just because of all the discussion around supply chain. With that in mind are there ways to better vet vendors or partners?

Chris Smoak:
That's a good question, Chris. I think there's no perfect solution just yet to this. I think what it comes down to is your good partnership, as I've mentioned. If you're trusting a third party organization with your sensitive data or your sensitive business process, I think it behooves an organization to consider talking to them more about how they handle and manage cybersecurity.

Chris Blose:
And even at the start of that relationship when you're talking about RFPs or that initial search and vetting process, are you seeing people ask more difficult questions about handling security threats?

Chris Smoak:
Yeah, absolutely Chris. We've seen quite a lot of that on the more technical side, you know, questions about whether you have a vulnerability management program, questions about frequency of patching. But more frequently, I've also seen it — and this is very interesting from my perspective — I've seen organizations seek to try to make sure that they perceive cybersecurity threats the same. That they're kind of compatible organizations with how they treat and work through cybersecurity related issues.

Chris Blose:
So that's external partnerships. Let's go back to internal factors for a moment. For a company, is there an ideal setup for cybersecurity, in terms of, how is it segmented? Who's on the team? What does it look like from an organizational perspective?

Chris Smoak:
I don't think there's a perfect answer. There are a lot of ways to really approach organizationally integrating cybersecurity, and what I'll describe today isn't necessarily best for your organization. I'll give you a couple thoughts on how to approach it differently though. So many organizations do have somewhat of a siloed approach. They have application security teams, they have infrastructure security teams, they have security architecture teams. And so for some organizations that works very, very well.

Other organizations prefer to distribute those security resources out into the businesses and other areas so that they have more security conversations more frequently at the beginning of a process. So as a business begins to think about a new way to serve customers, they may also have a discussion on threats and other cybersecurity-related items. At the root of really assessing cybersecurity risks, we really think about the threat model. And this is what I mean when I think about, thinking a bit more practically about how you approach this problem. The threat model really considers the threats and the safeguards that can be applied to mitigate risk.

Just to kind of set the stage, at the baseline, we all face the same threat landscape. Now not everyone experiences it the exact same way. Industry verticals, large, medium, small businesses see it slightly differently. Just as an example, when a bank assesses threats for ATMs, they may assess the combination of both physical and cyber-related threats. On the other hand, if you think about how you might assess mobile banking applications threats, they have less of a physically exposed presence. So you might think more on the cyber side.

There's a little bit of an art to apply to this process. And the more we spend time understanding those risks of any particular type of attack, the better we understand how to mitigate it.

Chris Blose:
Now you mentioned, obviously those conversations with executives and the board. When you're having those discussions, do you see common mistakes or misconceptions about cybersecurity?

Chris Smoak:
A lot of times I'll hear things like, "We're too small. We're not a big name. Why would they come after us?" Unfortunately, as I said previously, we all really face the same baseline threat landscape regardless of our business size or our industry. Think about a thief that goes house to house in a neighborhood, you're checking if all the doors and the windows are locked. If your house is in that neighborhood, your doors and your windows are going to be checked.

In the cyber world, there's something very similar. Your doors and windows on the cyber side are really being checked way more often than you think. And it's consistent across the board. Just merely being in the neighborhood, or in other words, being on the internet, you're gonna get some level of that. If you're big, you may have more windows, and you may have more doors and therefore would be a little bit more of a bigger target. You may also have maybe a more recognizable name, which may, you know, increase the likelihood. But even small businesses really can be prone to these types of threats.

I think you have to really be vigilant across the board. And as we've stated, it really doesn't matter how large or small you are. You really have a part to play in this process, and unfortunately, those threats are just as real to you as they are to your Fortune 100 businesses as well.

Chris Blose:
So let's say you are one of those businesses who has always thought, “It can't happen to us.” Where should you get started with thinking about that triad of people, processes, and technology?

Chris Smoak:
This is one of the most challenging answers that I have to give to some folks. And so, I'll give you a little bit of a framework to go on. It's really hard for small and medium businesses to have even one technology focused person, much less a cybersecurity expert. We all know it's challenging to find people in that space. There just aren't that many workers available. So really many businesses struggle to take action, even if they fully understand the risks.

One of the largest challenges for organizations we see is called social engineering. Just as an example, Chris, plainly what that means is exploiting people or employees through their emotions or their desire to help out. We commonly see this in the form of email phishing, phone calls, or even in some cases, in-person interactions. An attacker can call an employee, give them a sad story and try to get them to do something that they shouldn't do. We've all seen those emails.

You get an email that says, "You've just won $1,000." Or something that says, "You've had an HR violation applied to your permanent record." All of which elicit some form of emotional reaction, and they're designed to prevent the employee from really thinking clearly about the situation, which is, of course, what the attacker wants.

For this specific set of circumstances, focus on building repeatable training that helps employees see the risk and the value of understanding these types of attacks. More broadly, though, all of this can be overwhelming, as I said before, to an organization without support. So if you're one of those organizations, I would encourage you to look at ways to leverage managed services, or other cloud vendors to help take advantage of a partner's cybersecurity expertise and apply it to your business. JAs a great example, many cloud vendors offer cost-effective methods for using their services, and many of which include baseline cybersecurity controls that represent top tier technologies. Leverage those partners to grow the business and later, you may decide that it's time to grow your own in-house team.

Chris Blose:
I’m glad you’ve brought up ransomware and employee-specific attacks. Let’s talk about another type that attracts attention: the data breach. What can an organization do when faced with a breach?

Chris Smoak:
Absolutely, Chris, what I'd say is, consider all the items we've spoken about thus far and put those into practice. First, consider an assessment of where your business's cybersecurity maturity level is today. Set a target maturity, which is very important, where you want to be. Don't concern yourself necessarily with where the numbers are today. Really focus on how you get them where you'd like to be and what timeline you'd like to set to get there. Develop those core programs to identify, monitor, protect sensitive information within your environment, and understand where your largest vulnerabilities are to take iterative action on those gaps.

The key, Chris, here is really being very methodical, taking a risk-based approach. And tackle those biggest risk items first, work your way down. And with each iteration, you get more and more confident in your environment, and can convey that to executives and customers as needed. That approach, regardless of the technical pieces involved, really helps businesses see how they have a way to move forward. They have clear goals set in mind. And I've seen many organizations take that path, Chris, over a number of years and arrive at their target of maturity and feel much better about where they are, which can drive their, you know, overall confidence in being able to protect that information and keep themselves out of the news.

Chris Blose:
Ultimately, that classic triad of people, processes and technology offers a great framework for your thinking on cybersecurity. Equip the right people with repeatable, tried-and-tested processes for preventing or responding to an attack, and balance your technology spending where it makes the most sense based on your specific threat vectors.

Thanks to Chris Smoak for offering his perspective today, and thank you for listening. Get related resources for your business and listen to future episodes at regions.com/commercialpodcast. And subscribe to this podcast on your favorite podcast service.

Regions Bank, Member FDIC, Equal Housing Lender. This information is general education or marketing in nature and is not intended to be legal, tax, or financial advice. Although Regions believes this information to be accurate, it cannot ensure that it will remain up to date. Statements or opinions of individuals referenced herein are their own—not Regions'. Consult an appropriate professional concerning your specific situation.