INTRO:

Welcome to the Treasury Update Podcast, presented by Strategic Treasurer, your source for interesting treasury news, analysis and insights in your car, at the gym or wherever you decide to tune in. On part five of the #GoStrategic series, guest hosts, Alexa Cook meets up with Craig Jeffery, Managing Partner of Strategic Treasurer, to discuss why secure treasury is vital across organizations today. From a system perspective to organizational access and human elements, they share valuable insights on several layers of security. Listen in to find out how to protect your organization's assets against sophisticated criminal activities.

Alexa Cook:

Hi everyone. Welcome to the Treasury Update Podcast. This is Alexa, your host and consultant at Strategic Treasurer. And I'm joined today with Craig Jeffery, managing partner at Strategic Treasurer. Welcome, Craig.

Craig Jeffery:

Thanks, Alexa.

Alexa Cook:

So today we're going to be diving into the #GoStrategic series and we're going to be covering the topic of Secure Treasury. So Craig, why is security so important and why is a secure treasury something that has so much emphasis?

Craig Jeffery:

Yeah, that's a good question. I mean the goal of treasurers for example, is to protect the organization's assets, to make sure they have enough liquid assets whenever the time is necessary. And as the stewards of the most liquid assets, that's a vital element. And so when we think about security generally it might be protecting your liquid assets. It might be protecting data, as well as other resources, in addition to the reputation.

Craig Jeffery:

So security is really important because that's a core role of the treasurer. And why is securing treasury particularly important today? Two things that are driving that in particular, one, is the success of the criminals. They're having a great success in lifting data and lifting funds out of organizations. So the loss levels are higher, so it's more material. And then from the sophisticated standpoint, the criminals are more organized, they're more patient, they leverage technology and this sophistication is leading to a greater level of success and loss.

Craig Jeffery:

Therefore, to meet our needs, we have to be better on our defenses. And this one involves securing things from a system perspective, from an organizational or access perspective. And also from the human element, how do we ensure that people are doing the right things and not doing the wrong things that eliminates or could eliminate the different security layers that we have?

Alexa Cook:

Okay. That actually leads into my next question, which is, do you think that the human element of the security is on par with the technical side or is there room for improvement there?

Craig Jeffery:

There's massive room for improvement. We talk about those, the different areas about organizational, how do we organize our data and people. I think people are pretty aware of, Hey, we need a firewall. We need to put dual controls in place. We need to add a line that says this email originated from outside the organization. Companies are pretty good with that, but a very large percentage of organizations are not keeping up on the human side, in terms of upgrading the humans or updating their thinking about the different threats, particularly for payments and for treasury.

Craig Jeffery:

Training has been pretty good about anti-phishing training. Making sure you don't just click on links that come into your email box. They test those, but there tends to be far less adequate for understanding the different attack vectors that the different criminals use to compromise a platform or to ex-filtrate info or money out of an entity.

Craig Jeffery:

So no, I don't think it's keeping up. We have seen some really good progress in it, which is excellent. It's not keeping up on the technical side in our view and from the survey data we've recovered

Alexa Cook:

That makes sense about the human element. And I think that kind of leads into the next piece, which is payment security training. When I think of treasury payments, I think that's one of the most human touched piece of treasury functions. And so, what's the value of payment security training or even treasury security training?

Craig Jeffery:

Yeah, I like that question. So a survey we did with Bottomline Technologies showed that just about seven and 10 corporations train their employees on security on an annual basis. Now, not all of those are training on the payment fraud issue or protecting the payment process or understanding some of the key elements of treasury. But this is a big bump. There has been a growth in there. But still, if you said 30% of organizations don't have a firewall or don't lock their front doors, everyone would run around like their hair's on fire. And the fact that 30% aren't doing it and way more than 30% aren't doing stuff on payment security. This is still a big concern.

Craig Jeffery:

So what's the value in doing that is? I mean the human element is one of the areas where you can bypass other controls that are in the system. Business email compromise is spoofing people, getting people to think that they're getting instructions from an executive that says send money. It's not valid, but they think it's valid. And then money is being ex-filtrated out of the organization by people that should be protecting and inside the organization. And so, that's just one example.

Craig Jeffery:

And Barbara Corcoran from Shark Tank fame, her company had been hit with nearly $400,000 loss. Now, fortunately they were able to get to the German bank, their bank pressured them to say, give us time to prove that it was a fraud. They froze the funds and they were eventually able to recover those assets. But the point is, security training and treasury security training in particular, helps people understand what's wrong. You don't want to rely on people's, this doesn't feel right. You want them to know why something's not right and know what to do and if something goes wrong, how they can recover that. So they can apply the key 12 principles to their organization, to their processes and to what they do.

Craig Jeffery:

The value is almost inestimable for protecting the assets, but it's also a requirement in some cases. So if we look at card security, the payment card industry data security standards or PCIDSS, that's been in place a long time. And that requires a training element across the different roles of an organization. It's required that you be trained. And then more recently, just a few years ago, Swift CSP, the customer security program, required the same thing, training across different areas. So we see that and expect that continued to be required. But when you see these different payment platforms requiring it, you can expect that that should continue.

Craig Jeffery:

And why wouldn't you have training on this? Because of the level of losses. It's massive. The number of organizations that are suffering a loss, 60% have fraud attempts with losses in the past year. Fraud attempts grew 50% over a three year period. Those are massive numbers and people want to separate you from your money and from your data and the people need to be trained with current training and training that's relevant for payment processes and treasury in AP and payroll in particular as well as executives.

Alexa Cook:

So it leads me to my next question, which is what is secure treasury and why was it created? And I think in short, it's to kind of address some of the issues that you've walked through. But ...

Craig Jeffery:

It is. And so, we saw a few years back, we saw some gaps in training that's available for security purposes that are available through some of the different learning management systems. We also saw an increase in the requirements for payment processes like Swift CSP. And so we created a set of courses that covers a range of topics from the attack vectors, the principles of security, how to put those in place, different case studies that exist. How can we learn from those? Putting in place a defensive posture.

Craig Jeffery:

So we created that to help address this rapidly rising attack environment and increased level of threat and to also help organizations meet their requirements by being part of these payment platforms. And to make it harder for criminals to steal data and dollars. So that's really where it arose from. As we continue to look in this area, we saw a big need, a big gap, and wanted to do our part to help with that.

Alexa Cook:

Okay, so then what's coming out next as far as payment security trainings go?

Craig Jeffery:

Not too long ago we released the 12 key security principles and then we're rolling out a series of courses. I think it's six courses for PCIDSS. So that requires anybody who keeps card data, runs card data, there's a certain standards that are required to cover different topics. And so we've created a core series as part of the broader secure treasury environment to handle that.

Craig Jeffery:

And so, as we see this growing, we'll add, if there's things for, let's say, notch up puts out some requirements, we'll add to those. We want to make sure that we have a growing library of courses that are relevant to executives, those that are managing payments, those that are protecting the organization's assets so that they can, online, get some insight, take a test, make sure they're learning things well, retake it if they don't have it and then grow from there.

Craig Jeffery:

And so, that whole testing component we think is excellent. People take the courses much more seriously when they have a testing component and it's nice for the company, whoever is the admin to say, yep, everyone's been trained or these four people haven't been trained yet. We've got a month to go. They can be reminded their current and brought up to speed on what's happening and what they can do to prevent fraud or reduce the likelihood of that being an effective loss.

Alexa Cook:

I guess then just to recap everything, we've gone through, why security is important. And I think what I understood is one of the main pieces was that Treasury's goal really is to protect the liquid assets. And so security needs to be kind of at the forefront of Treasury's focus since everything's online and there's so many more fraud attempts. And I think you said that the success rate has increased by 50% over the past few years.

Craig Jeffery:

Fraud attempts. Fraud attempts has increased by 50%.

Alexa Cook:

So with the fraud attempts increasing by 50% and that's really the biggest driver, is those successes of the theft to just make sure that security is at the front of Treasury's priorities. And then the training course, Secure Treasury was created through the identification of different gaps in training and the increases in requirements. And so anytime that there's any new major requirement or rule put out, we plan to update the Secure Treasury, I guess toolkit, with a number of different courses there. Was there anything else you wanted to add to that?

Craig Jeffery:

Yeah. One thing I wanted to mention, we also, we ran some correlations of firms that train and don't train. We also ran correlations among a number of different elements of protecting organizations. And we have a podcast with Bottomline Technologies and Christopher Gerda on a number of those topics. But one thing, just to make sure this one correlation that makes sense is, if you have training versus not having training, what's the difference in terms of actually suffering a loss?

Craig Jeffery:

So if you have training, you have security training, what's the loss if you don't on ransomware? So ransomware losses five times versus those organizations that do have training. Business email compromise four times the loss experience, those that don't have had that training. Even payment diversion fraud and ACH fraud, 1.5 to two times greater level of loss, a greater frequency of loss for organizations without training.

Craig Jeffery:

So training the human element is a great way of reducing the likelihood that your organization will have a loss. The criminals are very sophisticated, relentless and automated and we need everything tightened from systems to our organizational access, to the human element.

Alexa Cook:

Thank you Craig for joining me today on the #GoStrategic podcast series.

Craig Jeffery:

Thanks for having me.

OUTRO:

You've reached the end of another episode of the Treasury Update Podcast. Be sure to follow Strategic Treasurer on LinkedIn. Just search for Strategic Treasurer. This podcast is provided for informational purposes only and statements made by Strategic Treasurer LLC on this podcast are not intended as legal business consulting or tax advice. For more information, visit and bookmark, strategictreasurer.com.