Stimulus Tech Talk Episode 16: When and How to Report a Cyber Security Breach: Expert Advice

Wed, Sep 13, 2023 8:25AM • 19:37

SUMMARY KEYWORDS

breach, information, report, customers, companies, local fbi office, communicate, insurance company, employees, cyber attacks, happened, builds, process, business, forensic, records, stimulus, blame, regulations, ceo

SPEAKERS

Nathan Whittacre, Sherry Lipp

Intro 00:00
You're listening to stimulus Tech Talk. A conversation based podcast created by Stimulus Technologies covers a range of topics related to business and technology.

Sherry Lipp 00:14
Welcome to a Stimulus Tech Talk. I am Sherry Lipp, marketing manager at Stimulus T echnologies. And I'm here as usual today with Nathan Whittacer, CEO of Stimulus Technologies. And we're going to be talking about how and when a business should report a cybersecurity breach. So we've talked a lot about preventing breaches and what and some steps to take and planning. But now we're gonna get into some specifics about what to do when it happens. So there's kind of a lot of different places, I think we could start, but we can kind of get started with who should Oh, and welcome Nathan, I forgot to say that. So to get started, who should cybersecurity breaches be reported to?

Nathan Whittacre 01:07
Well, I think most companies will not want to report anything. You know, that's, that's the initial feeling is like, oh, my gosh, this happened to me. I don't want to tell anybody because it can be embarrassing. You know, I, in one of my presentations, I talked one time about, you know, the fact that, you know, when you have a car accident or break in at your office, you know, there's no embarrassment of, you know, reporting a theft. But certainly, with cyber, you know, there's this stigma that you did something wrong. And companies don't want to report, but there are a lot of legal regulations that require you to report. So first off, you know, you got to know what, what governing body you're regulated by. So if you certainly if you have a breach, and you have some type of compliance obligation, you know, to HIPAA, or CMMC, or FTC, or what, you know, these different government organizations, they have requirements reporting, built into those regulations. So before you have a breach, you need to make

sure that you have a plan of who you need to report to, from a regulatory standpoint. But I can tell you that most states now have some type of regulation that require you to report data theft to your customers if their information is breached. So you kind of have to divide this up. Because if you have this internal information that's that's, that's breached without any client or confidential data, you don't necessarily need to report that to your customers or report that to government agencies. But if you have personal identifiable information, whether it's employee records, client records, anything that could be associated with PII, or Personally Identifiable Information, or Healthcare PII, those have to be reported per state law to those consumers or individuals. And so it's a complex landscape, because there's, there's a lot of different regulations. So I would say the first thing you'd want to do is discuss it with your insurance company, they're a good, good place to start, because they're going to know a little bit more about the regulations and who you should report to. Also, if you have a data breach, you can communicate with your local FBI office, they generally have a team that's assigned for cyber attacks, and they want to track these things down. And also, maybe your local police is a good start too and they can guide you. So before you have to communicate with like all your customers, you talk to the authorities first and they can guide you through the process. So don't be embarrassed, you know, it's like getting in a car accident or getting your office broken into, you know, start with the authorities. And then you know, same thing, contact your insurance company, and they'll guide you through the process, but there's probably a lot of reporting that you have to do beyond that, which can be embarrassing.

Sherry Lipp 04:33
If you do have a breach, like you're saying if it only affects your business, it's not a customer impact. Should you report it, even if it's not a legal requirement, just because it is a criminal activity and, you know, it could be somebody there tracking?

Nathan Whittacre 04:48
Well, I would certainly report it to the government agencies. I was just dealing with a prospect this week. And you know, we were discussing you know, there process that they've done. And they did contact the local FBI office. And they directed them to Homeland Security's CISA, which is a cyber attack group that's been developed under the Homeland Security, and they're, they're actively tracking these groups and trying to find them. And so working with these government agencies, you could potentially help bring down these, these groups. And so, you know, a lot of times, you know, the, these, the hacking, and the cyber attacks are not just individuals that are attacking and taking out businesses, they're, you know, groups of people, whether it's a state sponsored cyber attacks, or just a, you know, small group of individuals, they want to take these rings down, and they've, they've done a good job of tracking these things down. And so, you know, they want to be informed so that they can, they can do this. So don't be embarrassed, you know, that, again, you can search on the web, you know, your local FBI office, and I would say if there's any type of breach that you have, you know, get them involved, just like you would, you know, if you had a break in in your office, you want to report it to the right authority, so that they can find, find those individuals, hopefully.

Sherry Lipp 06:18
Are there companies who maybe don't report breaches, because they are worried that they're going to be blamed for it.?

Nathan Whittacre 06:25
Yeah, you know, that's, that is the common issue, why companies don't want to report because, you know, not like breaking into an office, you know, it's a perception that it's not your fault, you know, you have you've locked the door, you have maybe a security system in place, you know, you've done some things to protect your, your physical location, but there's this embarrassment of, okay, I was breached, maybe I did something wrong to invite that breach in. And you might have, I mean, an employee might have done something wrong, or, you know, somebody clicked on something. But you know, and in the end, you need some experts to walk you through the process. And that's not just your IT and security professionals, it's also, you know, some government authorities that are here to assist you through the process. And I would suggest getting your insurance company involved too, because they can help you find some vendors that can do some forensics on your on your network. And they if you have cyber liability insurance, they'll they'll pay for that for a certain amount to figure out how the systems are breached, and prevented it the future.

Sherry Lipp 07:38
I'm assuming, like with any crime, it's best to report it as soon as possible. But legally, how long does is there any legal requirement for how long somebody has to report it?

Nathan Whittacre 07:50
It is state by state, and I would recommend talking to an attorney or somebody about those. And it also depends on what type of information was potentially stolen or encrypted. It there's, there's a big shift there. And so having, again, talking to the experts, whether it's a attorney, or your insurance company, they'll help you through that process. Because it really depends on what information was breached, whether it was you know, payment, card information, healthcare records, maybe PII on your employees or your customers. There are different regulations, but you know, on those things, some of them you have to not just reported that help your customers potentially sign up for credit reporting services and pay for that. So there may be some things that you have to do, and you have to do it relatively quickly. It can't be something that you do years and in the future. So again, it depends on every state has, this is often regulated by the state, and every state has different reporting methods and who needs to report and then again, if you have, you know, protected information, it depends on the information that got out.

Sherry Lipp 09:06
And what information is a business going to report when they make the report?

Nathan Whittacre 09:13
Yeah, so they're gonna generally give the type of attack that happened, you know, their information that may have been released. You know, we've probably all gotten this letter for as a consumer in the mail at one point that, you know, your, your, your, the store that you regularly go to, or maybe a vendor that you use was breached. You know, they say estimated what happened when information got out and then what they've done about it. So there's, you know, we've seen these letters before, probably just throw them in the trash. But a lot of times if you're, especially if you're dealing with credit information, whether it's credit cards or social security numbers, date of birth, things like that for consumers. There's maybe some the Your requirements to pay for credit monitoring services as part of that. And again, if

you have cyber liability insurance, it might cover some of that. So that's why one of your first phone call should be to your insurance company.

Sherry Lipp 10:17
What requirements does a business have for reporting to their customers?

Nathan Whittacre 10:26
Again, it really depends on the type of information that got out. So you know, if you're, if you're a business to business, company, and you don't have any personal information, so if you just have, you know, information on your, your vendors, or your customers, business name, and mailing address, things like that, and you don't have credit card numbers stored, and none of that was breached, then there's probably little that you have to report. But if you're even if your business has been collecting, like bank account, ACH records, or, you know, tax IDs, things like that, then you would have to notify them of that information. So it really depends on the type of information you have. And if it's classified, you know, under a regulation of having to be reported.

Sherry Lipp 11:23
So how does it company kind of going back to like, this has just happened, how do they assess the exact impact of the breach on their company, and on their data?

Nathan Whittacre 11:34
A lot of times, you'll bring in a forensic expert that will go back and do the research on what what information was impacted, how it was impacted, and their, you know, their specialized companies that come in and do these forensic investigations. If you have proper insurance in place, a lot of times the insurance company will pay for that, and require it as part of it. So you know, they'll have a set of firms that they use in the different areas, and they'll come in and pull all the data on the network and information and, and do an analysis on it. So there's very specialized firms, these are, you know, forensic computer companies that will do that research. And the great thing about that, too, is that will also, hopefully let you know what you can do better on your network to be able to patch it so that it doesn't happen in the future. So we've seen, you know, again, as we've worked with prospects that come to us after a breach, we often work with this forensic company to implement new technologies inside their business to prevent future attacks. And sometimes companies have done everything that they can possible and and they're just, sometimes you can't be 100% accurate. So there may be little that you have to change. But those forensics companies can often identify where the breach happened, and then all the information that was, you know, part of that data breach.

Sherry Lipp 13:04
So if this happens to a company, and they've put out their notifications, Donal recording, how do you have advice for how they can, you know, do their notification to customers and can go forward and keep that trust or build that trust back?

Nathan Whittacre 13:21
That's probably the hardest part of it, you know, sometimes when these things happen, you know, creates this sense of lack of trust, you know, unlike go back to the example of your office being broken

into, you know, there's often very little blame that happens when, when your building is broken into, but when your networks are broken into, you know, the tendency that we have today is to blame the company. I think, if you over communicate, if you are actively communicating on what's happening, what what you've done to prevent it, I think it builds that trust back, hiding, you know, hiding the information or not communicating, it builds that lack of trust. So I recommend, you know, make sure that you have some written letters out to the customers communicate other ways via email, social media, whatever it may be. I was really one of our peers, that I know they're, they're not a customer, but they they had a breach. And I was very impressed by their amount of communication that they had they owned up to the breach very quickly. They let their customers know that they were going to be down for a certain amount of time as they resovled the breach. Throughout that process. They continued to communicate with their customers. They put some information out in the local media to to notify what had happened, and they you know, they continued to have that strong communication strategy of what they, what they did, what they're doing and how they're getting back up and running. And I think it built a lot of confidence back up, that they were willing to, you know, resolve that problem. So I think the more communication you have, the better if this comes out and you know, a local news report or social media or whatever, without you saying it, if you don't control the story and the narrative, then that's what builds that distrust for your organization. But if you control the narrative you're communicating, you're getting that information out there, that you can build that trust back up very quickly.

Sherry Lipp 15:32
Yeah, I think transparency in today's digital age, because we have such an easy ability to be transparent, it's very important to people, you know, that we that we will be the ones that communicate, it's puts us closer to the customer, although on both sides, both good, and you get the instant feedback as well.

Nathan Whittacre 15:51
Absolutely. You know, and again, with as being the CEO, the buck stops with you, you know, don't blame other people don't blame your IT department, or your, your vendors, or whatever it may be own up to it, and just, you know, notify everybody what you're doing. And I think the other thing that we need to be careful of is to communicate with your employees to what's going on, because, you know, they might be your customers, but they're your most important asset in your business. So, you know, communicate with your, your employees, let them know what's going on, oftentimes, their work is going to be dramatically disrupted, and, you know, show some confidence that they're going to have a job the next day too, you know, there's always that worry that, you know, if this data breach happens, we can't work today, you know, we're gonna lose customers, you know, exude the confidence that you're gonna get past it, and the employees will step up and help you through, but through it, too, don't blame them, you know, obviously, for what happened and and, you know, as a CEO, you know, take take charge and make sure that you get through that.

Sherry Lipp 16:59
And do you think it's important for business to have a plan for employees? If they get asked about this, you know, what their response should be? Or who they should direct people to is probably important?

Nathan Whittacre 17:12

Yes, certainly, I think having a clear communication strategy beforehand is really important. And make sure that that communication, no matter who you talk to inside the organization is the same. So the, you know, the distrust is seeded by misinformation or different information coming out from the organization. So there should be a central line of communication that's out to customers or to the media or whatever it may be, and it should be unified, you know, what that communication is?

Sherry Lipp 17:50
And, you know, I think this is important information for businesses, like you said, there, you know, they can be embarrassed to report it. Do you have any final thoughts on this on how businesses, business owners and CEOs can get over that fear of reporting this type of crime?

Nathan Whittacre 18:07
I think having a strategy before it happens is the most important thing. You know, it's probably for most businesses, it's not if but when you'll have some type of breach that you'll have to deal with. And so every business should plan for this, so that they're prepared and can move forward through an existing plan rather than having to come up with it on the fly. So the better you plan, the better you're prepared, the easier the process will be going forward. That's, that's probably my biggest advice is just spend a little bit of time on putting a plan together. There's plenty of companies that can help you with that. Stimulus Technologies sets it as part of our security packages. You know, if you're not one of our customers, maybe talk to your insurance company to get some recommendations. And there's plenty of templates online to build this but a good communication strategy. And disaster response plan is, is worth its weight in gold when it happens.

Sherry Lipp 19:16
All right. Well, thanks so much, Nathan. Great information as always.

Nathan Whittacre 19:20
Thanks, Sherry. It's always great to do this.

Sherry Lipp 19:24
Thank you, everybody.

Nathan Whittacre 19:27
Thank you.