Cyber Security Business - Episode 2: "At-risk Data and the Dark Web" with Chris Dunning, CSO, Affinion

Kevin Pouche: Hello and welcome to Cyber Security Business. I'm your host, Kevin Pouche, the COO of K logix and in place of Kevin West today we have Katie Haug our marketing director. Say hello to our audience.

Katie Haug: Hello, thanks for having me.

KP: As always, the goal of our podcast is to interview CISOs and other security leaders to hear their advice on the business of information security. This podcast gives our listeners actionable takeaways to help them increase the effectiveness of their security programs. Today we're joined by Chris Dunning, CSO of Affinion Group. Chris, thanks for joining us and welcome to the podcast.

Chris Dunning: Thanks. It's great to be here.

KP: So to kick it off, Chris, we thought you could give our listeners a little bit of information about your background, talk to us perhaps about how you got into information security, and maybe briefly walk us through your career. I think you've worked for some really interesting organizations and certainly some high-profile ones along the way.

CD: Sure, Kevin, thanks. It's funny, earlier today I was meeting with a new manager just starting out and the advice I gave him when he meets his new team and starts working, be sure to sit down and ask them their story because everybody's story is different and ultimately plays into how you work with them going forward. Mine started as a project manager, so I was working for a regional bank in Rhode Island doing data center implementation configuration in the mid-eighties. The interesting part of the story is one day I get a phone call to stop what I was doing and come to the VP's office and I walk in and there's a couple of blue suits and my boss sitting there and I get introduced and find out that they are external auditors and I guess they were able to debit the CEO's personal checking account at the bank one penny because of a lack of controls within the banking business process.

So that was my first project working to implement Rack F, which was a mainframe security tool for the bank and the interesting part of the story is I was given unlimited resources and unlimited money to get it done because this was going to have a direct impact on the bank's ability to operate as a bank. I completed the project, big pizza party at the end and went back to see my boss and said what's the next project? And he said we have to go see the VP again. So I walked back into the VP's office and they sit me down and they said, you're good at this and as of this afternoon you've been appointed the IT security manager for the company. And I said what happened to so and so? And they said so and so doesn't work here anymore. So I started to realize that not only is this an exciting dynamic field, it also can be very limiting on your career if you don't do it well.

From there I stayed at the bank. Before I knew it I was working for Bank of Boston and I became a regional security officer responsible for multiple banks and then had another opportunity to move over to the insurance industry. And I quickly realized I had a unique skillset and the fact that I could build security organizations because of my understanding of how security tools and technology got implemented within the business process. It just was a logical thing for me to do to build the people around it. So I went to an insurance company, at the time called Allendale. It's now FM global. I put their security organization in place and was there for about four or five years. And technology just kept changing. And the challenge that a lot of earlier and older security professionals had was the fact that you were limited by the technology you touched. And some of the organizations had leadership that wanted to silo that technology and didn't want to get full visibility. And there was this brand new thing called client server being developed. And I wanted to get involved with it, so I actually left there to go run disaster recovery and the service desks for Stanley Works in New Britain, Connecticut. Just wanted to do something a little bit different because I'd spent a lot of time in the data center space technology. And then in a meeting with the CIO, somebody mentioned I did security and two weeks later I was responsible for security at Stanley Works.

So it just became this thing earlier in the career, where you did two things, my background was data centers and infrastructure, but you also did security on top of that. And then I had a real good friend of mine who had been reaching out to me who had left Stanley and gone over to Staples and wanted me to come over and work in the data center space and lead that organization. And it took a year for me to get settled because of changes in my personal life. So between that time, I worked for a consulting firm that focused around HIPAA for a year. And then I also worked for IBM for about a year, and then finally made my way over to Staples where I became a director responsible for production delivery, which was the data center organization, but security was under it.

So this was really the start in the late nineties, early 2000's when security was starting to be recognized as a true leadership role that had to be recognized and report at the senior level within the company. Staples at the time was a very big company and it was buried kind of deep within the operation side. And this was just trying to get it higher up closer to the CIO. About two years into that tenure, things started to change, large scale breaches in the northeast. Everybody was talking about BJ's, which was down the road and all sorts of things happening. It's when a lot of the compliance requirements, PCI started to evolve from the CISP program into the true PCI program. SOC's was being launched and the CIO at the time said it was time for me to move into that role full time.

For the remainder of my tenure, about seven years, that's what I was responsible for at Staples through all different iterations of challenges from a business process point of view. But it's where I kind of really started to focus on this view with one of my coworkers, I'll give him a shout out, Ed Kelleher, who was really smart when it came to understanding the business processes. He taught me a lot and I've used that ever since as kind of my foundation for establishing any good strong security program within an organization. You have to understand your business processes, your business use cases for data and put appropriate controls in place and be smart about it so you're not wasting money and not missing the risks that you have.

I left staples in 2009 and I've done a few smaller companies which I really enjoy, all investor/VC owned that are all really trying to do something new and different and one of those first companies was an e-learning company. From there, moved into business services, call-center services, and dealt with 30,000+ plus employees and the challenges that come from people, to now being over at the Affinion group, which is one of the largest volume credit card businesses I've ever been involved with. I'm really focusing around the services that we provide from loyalty and travel and membership services as a third party to other very large financial institutions and other companies.

KH: You've obviously seen such an evolution take place from the start of your career to where we are now. How would you describe the current maturity of the CISO role and information security as a whole?

CD: That's a loaded one. So it's hard, because when you look at the evolution, has it gotten better? Definitely, but it's still a game of averages, we're gambling a little bit because there's no way to be 100 percent secure. If you're going to be 100 percent secure, you're going to have everything locked down so tight that you can't be in business, you have to have some amount of sharing of information with your customers, with your vendors and third parties that you work with, with your employees. Risk is one of those things that you truly need to understand and manage to. I think it's gotten much better. I think we understand risk much better than we ever have in the past.

The other thing I think that the industry has done and I say that both from an information protection and from an information technology point of view, we understand where all the big risks are and the low hanging fruit. I think that's why so much focus has been placed on credit card data and our ability to use that and protect it. What's happening and I think everybody sees this happening now is governance and laws are being put in place from a privacy point of view that are creating complexity that aren't necessarily managing to risk but managing to the expectations of the people that live within the countries where those laws apply. And we have to stay focused on how we lace that into business because you see people having trusted relationships with the business and opting out and sharing their information which is how it should be. We have the ability to share information, but recognizing that once we have that information, we have a duty and a responsibility to ensure that it's truly protected.

KP: You kind of bucked the trend in terms of you were a CISO before there was a CISO title and you came up with a business focused background for a security leader. Whereas the trend we tend to see is coming up the ranks from a more technical role. Does the new CISO of today and tomorrow require a more business focused leader?

CD: So one of the things that I was involved with a few years back was a Dartmouth University School, the Tuck Business School has an executive ed program and I worked with a couple of the directors there to provide input to a program that they were running which was the business essentials for the information security professional. And the focus there was how do we give those mid line manager individuals the level of understanding that they have or they need going forward because they've got the technical skill. A lot of these people came up through the engineering ranks and what's the best way to ruin an engineer is to give them a management title. Now he can't do the thing that he loves and he's going to deal with this person not showing up to work and the various pieces and parts that go with that versus taking somebody who's in a management role who is technical and getting them to be a security leader.

You've got to understand the financials and how they apply to the company. You've got to understand risk and how to measure it and define it. You've got to be able to speak the language of the business. You have to be able to turn off the technical speak and I sometimes call myself a translator. I sometimes call myself a fixer, but the reality is if I get a room of very technical people together, I can talk to them and then leave the room and then go talk to the C-suite and say, this is what that translates to from a risk point of view and what it translates into from a business point of view and getting more of those leaders lower in the ranks is just very powerful because in the day to day decisions that they make, you can have a level of confidence and comfort that they're not just doing technology for the sake of technology, they’re constantly taking the business for you.

KP: Why don't we switch gears and talk about the dark web and what it means for at-risk data in organizations. Starting at a high level without getting too deep, what is the dark web? I think there could be a perception that the dark web is some individual technical people sitting in a basement in four corners of the world, or is this a more sophisticated operation with networks of people? And in some instances even nation-state sponsored, what's your view of the dark web and why is it such a risk?

CD: The risk has been there for a long time.

KP: Just an old problem with a new name.

CD: Long, long time. I've had opportunities to work with law enforcement both at the state and the federal level for many years and it's always had the focus of partnership and our ability to help ourselves is very important. One of the things I say to people all the time is, especially in security incident and breach response, wherever you're located, there is a local field office for the FBI or the secret service. Look them up online and get the number, call up and ask to talk to the agent in charge for investigations in your area. Establish that relationship so you have it.

I'll go back to the Clinton era under Janet Reno. I worked a case where we had a contractor working at a company I was at who was arrested over the weekend on a Sunday. And we found out about it because his name and picture were on the front page of the Sunday paper. So imagine having to show up to work Monday morning and have to go talk to the management staff that somebody who works in the building, not necessarily an employee, he's a contractor, but somebody who was working in the building was just arrested by the FBI and had a record for hacking. What do you do next sort of thing. FBI came out to the office, worked with us and things started to make sense, we found out through the help desk that some equipment had gone missing. We had found out that he was trying to set up a file share service for his family on our network. Just all different things.

Short version of the story is he was a young kid who was working off of let's just call them hacker sites, sites that are specifically set up by likeminded individuals to share information, tools and technology on how to hack. And he was frequenting himself there. We walked him out the door, provided the evidence to the FBI, and he got a year in federal prison. 25 years ago, his ambition was to become a great hacker, not to steal anything, not to gain value or money. Today it's very different. Today, it is nation-state funded, it is in certain parts of the world where individuals see a better career path by taking that route and they are actually recruited to do it and they can make less money taking the legal route or they can make lots and lots of money taking the illegal route.

Now is that the majority of the population? No. But companies like Russia and China have very active programs where they're looking to find what they can about us. China's a little bit different, China is a country that looked to grow and evolve through taking of information and that's well known and for years they've been doing it. What a lot of people don't know is the amount of support that the government places into everything to do that. One of the opportunities I had was to spend some time with an individual who was a former high-ranking person with the Chinese government and who left and defected to the US and shared the fact that their entire philosophy was to just steal everything that they could from us.

And in most cases we made it easy because as a country, we don't recognize that philosophy or belief that that's the right way to do it. There's also this value that comes from information and we've talked about this before, where the focus around protecting PII and protecting credit card and health information. There are different regulations like PCI and HIPAA and GLB and now a lot of the specific requirements coming in from Europe through GDPR. But the reality here is a lot of companies that they actually look closely at their business processes, they'll see that there's other types of data that can be immediately turned into cash and call it the dark web, call it subversive websites, call it just bad people that have access to do those types of things. Everything from your driver's license number to your loyalty cards has value and can be sold immediately for cash.

KP: So how do you quantify that risk into dollars and can you give us maybe a use case into just how devastating this could be to an organization?

CD: The company that I currently work at, we're a large loyalty company and gift cards are part of the program that actually provides services to our customers and our clients. At the end of the day, it's common for the bad guys to look for business processes that they can manipulate. Most companies say we want to be on LinkedIn, we want people to see our company, we want to see that this is a great place to work. It's a great place to recruit people. I need a specific database developer, I need somebody that can do marketing. Well, let's go look on LinkedIn. Let's see if we can find somebody and ping them and see if they're interested in a job. Never mind the whole LinkedIn job market services that they offer as well.

It's common for everybody to say I'm Chris Dunning, I'm the CSO at the Affinion Group. Well, what happens if you say I'm John Smith and I'm responsible for very sensitive data that's worth millions of dollars, but I don't say it that way, I say it that I'm a procurement manager. Well next thing, if I'm a bad guy, what I'm going to do is I'm going to start sending phishing emails to that person so maybe I can download remote control software and take over his PC and see what he really does, how he does it, and then ultimately manipulate and steal things that are worth thousands if not millions of dollars. And that's a very vague way of saying that's a very common thing that happens across a lot of industries. Look at the number of phishing emails that you get, and the reality here is every company, every mail service has very sophisticated scanning that looks for all that and filters it out.

So if you really think about it, the ones that are coming through are the ones that are most sophisticated, number one, or have been specifically targeted at you. They know who you are, they know what you do and they're trying to trick you into giving it up. And that's very different than what it was 25 years ago. I tell people all the time, you don't have to be a victim, but you have to operate it at a pace and a speed where you can be wise enough to understand that you could be the victim and that's a very important distinction to make.

KH: So when you talk about business process, where does security need to come into play? Should it be in all business process discussions? How does a CISO get to that point where they know they're truly part of the business process?

CD: I'm very lucky in the current organization I'm in. I own multiple facets of that process. The other part of it too is I did dual roles here for a few years where I was also the VP of IT infrastructure for the company. So when you look at security and technology infrastructure, they are truly integrated at this company. I've since stepped away from that role. We appointed a new VP of technology, but the information protection requirements are really laced into the technology. I also have governance compliance under me as well, which it should, but what we did is we created a new organization that we call data governance and I like to call it the high risk data discovery team and it's their job to actually go out and look for and to review business processes that might be at risk.

Often we do samplings when it comes to audits. We don't look at everything. When we look at high risk data discovery, we look at everything. So you know, looking at any type of process that takes payment, that gives money, that gives data that could be turned into money, talking a little bit about what their value is. You know, everybody knows credit cards are attacked and searched for within companies when they have incidents or breaches. What they're looking for and what PCI was really developed to protect, it wasn't the single transaction, it’s the large store of credit cards. The bad guys aren't going to take the time and effort to steal one card. It's too risky. It's too much work. There's just no return on the investment. But if they can get to a file that has 50 million credit cards in it, they've hit the goldmine.

Well what happens if they get a file that has 50 million loyalty accounts? Well, if they're smart enough to figure out the business process, they could figure out how to get to those loyalty programs and start booking travel and start turning that into gift cards or what’s to say if they break into some biomedical company or some health services company and they download millions of medical records and those records include prescriptions for some opioid and they find a way to manipulate the business process to then turn that into medications that they are able to sell or steal. I don't know what the risk is. I do know that if you don't know what your business processes is, you’re at risk. And to compound that, if you don't know the business processes that use data that can be immediately turned into cash on the web, then you are blind.

KP: So that's where you start understanding the business process. Is that the recommendation you would give to a new CISO that doesn't know where to start?

CD: Yeah, and I'd go in, based upon his business and what he does, figuring out where are the large stores of data and how are they used within the business process and based on those data types, what's their value? And really look at it through the lens of: if I was a bad guy and I was getting to get hold of this data, what could I do with it?

KH: And then what about when it comes to getting that mind share with the board and executives? How does the CISO then communicate the importance and the value of that?

CD: We have a program, our incident response program at the company, we call it the first 48, it’s a great way to market and promote the effectiveness of security incident response. When you talk about security incidents, it sounds kind of cold and kind of ridiculous because who wants to hear that somebody got locked out of their computer or somebody was dumb enough to leave their computer in the back seat and it got stolen.

But the reality here is the first 48 is really designed after the law enforcement's homicide investigation process because it forces the team to respond and provide as much information as possible around the event within 48 hours and then you make a decision, it either becomes a larger event or you shut it down so you don't waste the team's time. But what it also did, it went from most organizations. Every company I've ever gone to work for, the first thing I asked the team when I walk in is, show me your monthly security incident report. And I think 90 percent of the companies I've worked at, the response I got was “we don't have security incidents so we don't have a report.” And then usually two months after being tenured into the company, we've got a report that's running between 50 to 100 events a month and those are small security incidents but they give you the tone of what's going on, where you're seeing five things happening here, that might be a bigger issue that you're not seeing over there, you know, that type of situation.

I think that plays a big part into understanding the risks, pieces, and parts that you need to focus on more than anything else. I'm trying to remember the original question because I was going somewhere. That becomes a quarterly report to the board and it was so interesting because I'll go in once or twice a year and I kind of present to the board on specifically the annual strategy for information protection, whatever issues have come up and kind of what we're dealing with from a risk point of view. But they always want to talk through some of the specifics of the incident report. I didn't know that it’d become this really interesting topic at the board meeting where I could go in and I could add some kind of color behind some of the events and what had happened.

Originally, I wanted it so that I could present to the team those types of things that were creating certain scenarios that might have been bigger issues. The board took it, looked at it, and saw the same thing and wanted to understand what the implications were either from project, priority, or funding.

KP: You gave an interesting example earlier of somebody potentially spear phishing via Linkedin, a procurement person. I know you're a big advocate of internal security training and awareness. So is that part of your overall strategy when thinking about how to better protect yourself from being a victim of data theft on the dark web?

CD: Yeah, I think a lot of it comes down to how often and how creative you are. We have this thing called the awareness calendar and it's a calendar that gets published after the fact. My expectation was that we do so many things that there's no way we can keep track of all the awareness things that are going on, that on a monthly basis we have to create a calendar and show on each day all the stuff that happened so that we can look at that and say, okay, we're not doing enough consistently through the month. We're doing too much at the top, we're not doing enough, we missed two weeks, what happened? Those types of things. But it has to be real. It has to be real time. We use the PhishMe tool for phishing.

If somebody gets something, they just click on it, the mail goes away, it gets logged, it goes to the incident response team and they manage it. Previously we’d tell people if you had a phish happen, you call the service desk, and that's not going to happen. And then what to do, don't touch the email, don't do anything with it, the PhishMe link takes the email right out of their mailbox. All the risk goes away and we can respond to it. The other part of that is we actually run our own internal phishing against our own people using the same tool. So we'll create the phish, we send it to them, and then we measure: did they read it, did they open the attachment, did they click on the link, you can see just how bad it was and then appropriate training. It's something you have to do a lot.

And when I say that, it's gotten to the point where, and you can say this is good or bad, we do an announcement about a new service or product that's coming out, it came from the service desk and everybody's clicking on the PhishMe button saying this is a phish and it's a legitimate email. Well, it's just as easy for them to send out a notice saying it wasn't a phish and there's the reasons why, they can get back to the people directly and let them know. So it's a challenge. It really is.

And I’ll give you another interesting story. We had a phish that had happened within the organization, same type of thing: HR, click on this link, we need you to provide this information and he came to understand that the people who responded to it, they responded differently based upon their culture.

So what we found was, certain phishing attacks, if you were American born, and our office is based in the Stamford area, so let's just say a lot of New York City culture and if HR wants you to do x, y, and z, the first response was: I'm too busy. Why are they asking me this, they should know, and they just ignore the email. If you are a two-language citizen born out of the country, came here sometime during your life, you see authority different. And we had several individuals, all in that case, three of them, who responded to the phish because they thought: HR was asking, they're an authority, I have to give them the information. So we started to tailor the training to actually tell all employees no matter where you're from, what country you originated from or currently work in, because we're all over the world, no member of management, no member of HR would ever ask you for a password. And we had to reinforce that over and over again because they saw authority as different.

KH: And in terms of metrics, do you collect on average so many people clicked this month versus this month and are able to show to your executives or just your team, here's how we're improving. And then along with that, what about benchmarking against similar companies in your industry with their phishing rates? Does that occur?

CD: No benchmarking. And the challenge that we often have is, which industry do we align to, we provide services for banking, but we're not a bank, so we tend to fall into the financial services space. But we do do the first part which is, we do it by department. We phish a whole team, based on their results, they get re-phished, based on their results. So each time, based on their results, is certain things that happen. So if you opened the email, clicked on the link, you get training. You opened the email, clicked on the link and gave up your credentials, you get a one on one session with a trainer trying to understand what you were thinking and create a moment that hopefully you'll think again instead of just saying, oh go take the training course.

Second training, they do it to them again with a different email and if they fall for it, again, it's a person that goes out and tries to figure out what's the disconnect. It isn't about yelling at them. It isn't about firing them or getting them in trouble. We've got to understand because we've figured out something that if the bad guys figured it out, you'd give up your credentials every time and usually by the second time they get it and they actually become the advocate for this and are very vocal around the organization about what they've learned. You got to spend some time figuring out the why. Why did they do it?

KP: We talked earlier and you kind of started part of the conversation in your career, talking about some of the first most prominent breaches, right? People point to companies like BJs and so we also talked about how the dark web is really just a new name for an old problem. People certainly have gotten more sophisticated. I think companies have also gotten smarter, right? Security, as we've discussed today, has become more prominent. By and large, corporate America, are we more secure today than we were yesterday?

CD: I think we're trying to evolve as security challenge evolves. We're only as good as the risk that we know and understand. I love to say there’s an A, B and a C. There has to be a level of effort that's consistent and remains consistent for the ever-evolving risks that are happening. Who would have thought that a foreign country could have weaponized Facebook into manipulating people's behavior, right? A lot of people focus on a lot of the risks that's happening within our worlds today. Talking about different tragedies and events that have happened and that's the closest I've seen to a 9/11 level cyber-attack to many countries. We weren't the only ones that they've done and done that level of manipulation and I think everybody's seeing right now how that's continuing to the point where Facebook is saying we need help. These guys are really good at this.

KP: Well said. I think we're about out of time. Chris, we really want to thank you for joining us today. I think our listeners will benefit from a lot of this information, so thanks for joining us. As always you can find more about this and other podcasts on our website, klogixsecurity.com/podcast.