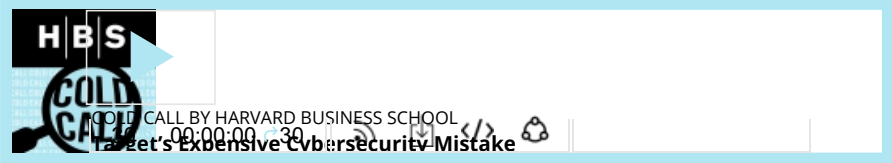
21 DEC 2016 COLD CALL PODCAST

Target's Expensive Cybersecurity Mistake

There is a joke in the cybersecurity community that there are two kinds of companies: those that know they've been hacked, and those that haven't found out yet. The Target Corporation learned this the hard way during the busy holiday season of 2013, when 110 million customers' information was compromised. Professor Suraj Srinivasan explores one of the largest cyber breaches in history, analyzing why failures happen, who should be held accountable, and how preventing them is both a technical problem and a matter of organizational design.



Subscribe on iTunes Follow on Libsyn

TRANSCRIPT Brian Kenny: Good news! In 2015, the number of data breaches in the United States decreased by 2 from the prior year. It went from 785 to 783. Now the bad news: the number of records exposed containing personally identifiable information doubled from 85 million in 2014 to 170 million in 2015. That means names, Social Security and driver's license numbers, birth dates, medical records, and other kinds of personal information in the hands of nefarious individuals. The fact is, the likelihood of your identity being stolen is doubling year over year, as major financial and retail institutions continue to be targeted. Whose job is it to protect your information? Today, we'll hear from Professor Suraj Srinivasan about his case, entitled "Cyber Breach at Target." I'm your host, Brian Kenny, and you're listening to *Cold Call*.

Suraj Srinivasan teaches in the MBA and Executive Education programs at Harvard Business School. His research examines the institutions of corporate governance in the U.S. and internationally. One of the many areas he studies is the reputational consequences for corporate directors when companies experience financial reporting problems. Suraj, thanks for joining me.

Suraj Srinivasan: Thank you for having me.

TRENDING

03 JAN 2018 SHARPENING YOUR SKILLS
5 CAREER-RELATED NEW YEAR'S RESOLUTIONS (AND 5 TIPS FOR KEEPING THEM)

02 JAN 2018 RESEARCH & IDEAS
THE MOST POPULAR STORIES AND RESEARCH PAPERS OF 2017

20 DEC 2017 LESSONS FROM THE CLASSROOM
HOW TO DESIGN A BETTER CUSTOMER EXPERIENCE

02 OCT 2017 WHAT DO YOU THINK?
DO BITCOIN AND DIGITAL CURRENCY HAVE A FUTURE?

03 JAN 2017 RESEARCH & IDEAS
5 NEW YEAR'S RESOLUTIONS YOU CAN KEEP (WITH THE HELP OF BEHAVIORAL SCIENCE RESEARCH)

FEATURED FACULTY

SURAJ SRINIVASAN

Philip J. Stomberg Professor of Business Administration

CONTACT
Send an email

Kenny: Could you just set the case up for us? What's the situation?

Srinivasan: In December of 2013, retail giant Target revealed that it had been subject to a massive cyber breach, which at that point, at least until then, was the largest breach of that kind. Between Thanksgiving and December 15 or so, Target was subject to a hacking attack. It had lost 110 million customer records that included the kinds of things that you just talked above: credit card information, personal identification, email addresses, name, home addresses, phone numbers, for about 110 million people. This led to a big reputational loss for Target, congressional inquiries, lawsuits, regulatory investigations, and the board was held accountable for negligence.

Kenny: We're going to get into all those details. I personally remember when this happened because I had just shopped at Target. This was the holiday season. Everybody was out shopping. Target is the place where everybody goes and I remember thinking, "Oh, gosh. Did they get my information?" I'm sure a lot of people that are listening can remember this, or the one that happened at Home Depot. This is happening more and more frequently. What prompted you to write the case?

Srinivasan: We teach a set of governance programs for boards of directors in our Executive Education every year. Cyber security is high on agenda for boards of directors. I used this case to help directors think about the challenges companies face when dealing with cyber risk management and what the board's role is in overseeing this risk. The joke in the cyber community is that there are two types of companies: those that know that they have been breached and those that don't know yet that they have been breached.

Kenny: Scary stuff.

Srinivasan: Cyber breaches are one of the biggest and most common risks that companies face today. Any large company faces hundreds of cyber-attacks every day. Companies like Amazon, I'm told, face more than 5,000 attacks every day. We wrote this case as a vehicle to learn about organizational issues involved in risk management of this sort; why failures happen, what the board and managers can do to better manage this risk. On the one hand, it's a technical problem, which needs a technological solution. On the other hand, it's an organizational design problem. It's a problem of resource allocation, one of creating an internal control mechanism within the company that can help them keep on top of a highly technical, but also a fast-changing risk environment.

Kenny: This case was written from publicly available documents, I assume. When we do cases here, lots of times you're in the board room. You're actually meeting with the protagonist. Is it more challenging to write a case this way?

Srinivasan: Yes and no. In a case like this, when organizations have been involved in a major incident, a negative incident of this sort, there is a natural reluctance to talk about it. Oftentimes because they are facing

→ More Articles

FIND RELATED ARTICLES

CRIME AND CORRUPTION

CRISIS MANAGEMENT

NATIONAL SECURITY RETAIL

lawsuits or have just settled lawsuits, there's a reluctance to talk about this. The flip side is, you can't get the firsthand information and you don't know whether what you are getting is the best possible information. On the other hand, because companies are naturally hesitant to having a harsh light shining on them, we face no such constraints when we only rely on public sources. In this case, it so happens, because of the large number of lawsuits, the media focus, the congressional inquiries, Target's own special litigation report, there was just a lot of information available publicly.

Kenny: I was really interested in reading the case to see the long history of Target. For some reason, it only came into my consciousness when I started shopping for things, but they've been around for a long time.

Srinivasan: More than 100 years, as Dayton and Dayton-Hudson. The origins go back to 1902, in Minnesota, when Dayton Company started a department store. After a successful run for about 60 years, Target was opened as a discount store, also in Minnesota, in 1962. That year, it turns out, was the golden year for those kind of stores. Walmart started the same year, in Arkansas, and Kmart started the same year in Michigan, the three giant retailers of the past 50 years or so. By 2000, Target had become the biggest division within the company and Dayton-Hudson changed its name to Target. The department store culture has stayed in Target from the very beginning. It's in the DNA of the company. While Walmart has always had this “pile it high, sell it low” model, their slogan for about two decades was, "Always low prices," if you remember. Target's slogan has been, "Expect more, pay less." They're known for good store ambiance, you obviously shop there.

Kenny: Yeah, my mother calls it "Tarjay."

Srinivasan: Exactly, that's the French Target, emphasis on design and innovation. You'll see designer labels at Target. To bring their department store ethos to discount retailing, and this has really served them well while competing on price with someone like Walmart. They're one of the rare companies that has successfully not just survived but thrived while competing on price with a company like Walmart. In the Amazon era, all bets are off on what's going to happen in the future, but Target has shown us how to be very successful and grow while also competing on price. A very successful company.

Kenny: Also, they've attracted a more upscale shopper as a result, and they call their shoppers "guests." All of this, to me, leads back to a situation where the breach and the way they handled the breach, which we're going to get into shortly, it was almost worse than it might have been if it had been a real discount store, because you get what you pay for kind of thing, but Target had built up expectations among its customers.

Srinivasan: Customer experience was very, very important for them. Ironically, their credit cards were part of the customer experience. I, by the way, wrote an earlier case on Target about six or seven years ago, under an activist situation, and a big learning that came out of that was that the

credit card business is a very important business for Target because they learn about customers that way. That customer relationship was very, very important for Target.

Kenny: Yeah, so let's talk a little bit about the attack. Can you describe, without getting into great technical depth, it was a malware attack. What was that? How did it happen?

Srinivasan: In the fall of 2013, one of Target's HVAC suppliers, a vendor-

Kenny: That's Heating, Ventilating, and Air Conditioning, if you didn't know the acronym.

Srinivasan: One of them got a standard phishing attack. All of us have gotten emails with an attachment that we are all advised not to ever click and open, if you don't know the source. One of Target's vendors got such an attack, one of the employees opened that attachment, and the vendor got infected. Using that vendor, the hackers got the password for the vendor, which let them access Target's internal network. Then they loaded this malware called Citadel, which allows hackers to scrape information whenever a credit card is swiped, even before Target encrypts the data. Basically the hackers collected magnetic strip data whenever a customer swiped a card at a store.

Kenny: Like at the moment that it was swiped, they were getting that data.

Srinivasan: Exactly. Though, as the attack developed, Target's weaknesses in their network security also let the hackers move around within Target's network. Target didn't have the right kind of firewalls. It should never be the case that a vendor is able to access payment information. Not only was the malware at the point-of-sale terminals, the hackers were also able to access other parts of Target's network.

Kenny: I thought this was amazing. They were able to actually update the malware multiple times while the attack was happening, over a long period.

Srinivasan: The initial entry into Target happened on November 12, it seems, but they didn't do anything until the day after Thanksgiving, which, as you know, Black Friday was one of the biggest sales days of the year. The timing was so well-planned, I must say. Unfortunately for Target, that period is such a high intensity shopping period and for whatever reason, the multiple alerts that Target was getting were not acted upon. Also, keep in mind, there are hundreds of special alerts getting created every day, but for some reason, a lot of the malware detection and deletion functions in their software seem to have been turned off. A lot of alerts that they were getting from their security protection system were not heeded at that point. In hindsight, there were some organizational reasons, some silos within the organization, that seem to have contributed to this, but yes, you're right, the network security was so weak that it let the hacker roam around freely for about two weeks.

Kenny: The total number of records they ultimately were able to get to was in the vein of about 70 million.

Srinivasan: Seventy million, where they lost the customer information; 40 million, where they lost the credit card information.

Kenny: That's just astonishing. How did Target handle this? After everything, after they revealed the information, reluctantly, what happened?

Srinivasan: To just back up a little bit on that, Target actually found out from the FBI on December 12. The FBI and the Secret Service had noticed a huge increase in the black market in credit cards. The common element in all of them was that they were coming from Target, that they had recently been used at Target. The FBI alerted Target and one of the learning points from the case is, what do you do when you get alerted? What do you do when you find out? Target took about three days to identify exactly what was going on and, once they did it, it took them about 12 hours to remove the malware. It was about December 15th by the time they could clear their system. Mind you, all the time, customers are still shopping and losing their information. Unfortunately, the nature of the problem is such (and Target is such a widespread organization with thousands of stores) that it takes a while to deal with this problem.

What is surprising, though, and probably points to some control weaknesses inside the company, is that the CEO was told only three days later, December 15. Again, we don't know exactly what was going on inside, but to me it suggests some silos and internal control problems when the CEO is not told of an FBI alert of this magnitude for three days. The board was told on December 18, another three days later, which again points to some communication breakdown within the company because by that point the media was coming to know because a prominent blogger had already started talking about this, all the banks were finding out. They cleared the malware on December 15 and then they have to get up to tell customers and set up the phone lines, find out exactly who is getting affected, and so on. They did that on December 19.

Kenny: So we're talking five weeks now into this attack.

Srinivasan: Yes, about five weeks into the attack, a week after the FBI has told them.

Kenny: People weren't happy. Customers, banks, all the people that were affected by this were unhappy with the way they reported it.

Srinivasan: Absolutely. There are hundreds of banks that have issued credit cards, some very small banks, community banks, which might be getting hit by their customer shopping there as well. Not all banks are equally equipped to deal with these kinds of things. Of course, Visa and Mastercard are the big payment processors and they're very, very unhappy when something like this happens. Some of the customer stories are so unfortunate, especially because it happened during the holiday time. There were people whose credit cards get locked up and can't do their holiday

shopping, can't travel for the holidays. There are families where they couldn't, come the new year, pay school fees, things like that. You very well know, it is very hard once your identity gets stolen in any way to then go and deal with all kinds of institutions to remedy this. Some of these stories from customers that came out are pretty unfortunate.

Kenny: This gets to kind of the heart of the case, which is all this has happened, who is accountable? Can you talk a little bit about the investigations that ensued and the trail that that leads back to Target?

Srinivasan: One of the things that comes out of this is: how do you set up the organization to deal with a problem like this? As I mentioned just briefly, just a little while back, it is a technical problem, so there are technical solutions to it, but also, how does an organization set its technology and its people up to be able to manage an issue like this? There were three different parts of the organization that were responsible for cyber security. In other words, no one was directly responsible for it. It was the CFO's office, the general counsel's office, and the Chief Information Officer, the CIO's office. All three had various roles to play.

One of the things that comes out in the special litigation company report is: how are these different parts of the organization talking to each other? If you have to create a committee whenever something like this happens, that is not a quick way of responding to something like this. I don't know exactly what the details were or how they were organizing internally, but it just seems, at least with the benefit of hindsight, that organizational issues were not set up in a way for speedy response to a problem like this. Then, of course, the technical issues that we talked about, or vendors' access, should not extend to payment systems. There's no need for a vendor's access to extend to payment systems. It's very common, I'm sure, if you have a bank account these days, you do multifactor authentications. You get a text message with a password that you didn't, or the code that you didn't have to put in. That is already a part of the payment card industry data security standards, the PCI DSS that every retailer has to undertake, but somehow that wasn't the norm at Target, at least as far as this vendor was concerned. There were infrequent passwords, the alerts, the second factor authentication alerts that were going back to them.

To be fair to Target, they had just then, actually, undertaken a PCI DSS compliance audit, but this also points to the fact that these audits may not be doing as good a job when the threat is so fast-moving. For example, if you do an audit, you're supposed to do one every year. You do an audit of the store and then you add a new software to your system, you reconfigure your firewall, the whole thing is now—it's not clear whether you've opened up yourself to some other kind of a breach. It requires a technical solution, but it also requires an organization that is designed in a way to be really fast-moving of this sort.

Kenny: And people who were qualified. There were some questions about the qualifications of the Target CIO, who came up through a different channel.

Srinivasan: Absolutely. She was a merchandiser. Given the kind of technical knowledge this area required, afterward they replaced her and brought somebody else in who was much more cutting-edge in terms of this technology, but that also perhaps points to the kind of attention that was being paid to this area. It points to a very important fundamental issue in something like this. If you think about the kind of talent that's needed for managing this kind of highly technical risk, that talent is going to go work in Google and Microsoft and companies which are in the technology area. You're not going to find themselves coming to a University, even, a cyber security or Chief Information Office or retailers, hospitals, but these are the places that need it the most. It is a big problem and organizations need to figure out how to staff, how to manage the staffing, how to manage the resource allocation in something like this. This is one of the big learnings you get out of case like Target.

Kenny: Let's talk about the board because the case goes into great detail about the scrutiny that the board faced in the wake of all of this. What's their role and responsibility?

Srinivasan: Absolutely. The board came under a lot of scrutiny after this. There were investor lawsuits that alleged that the board was negligent. Some of the congressional hearings, the senators and the congress-people were also unhappy with management and the board. Absolutely. It's a big issue for the board. Did they put the right process in place? Was there adequate accountability within a line of sight on who was managing this issue? Was there adequate talent on the board that understood these issues? What we try to do in the program is to think about a framework, based on a list of questions, that boards should be asking to keep on top of an issue like this. It is not reasonable to expect that every board is going to have highly technical experts on this and it's also not probably necessary to have highly technical experts on this issue, as long as there is an awareness on the kinds of questions that one needs to be asking.

We think about it as a framework, where you can start thinking about what should be the risk assessment. What should we be doing in terms of asking the right set of questions on risk assessment? What's the process of managing cyber risk in the organization? What are our most valuable assets and how vulnerable are they? How is the company assessing these vulnerabilities? How often should you assess these? Who should be assessing these? Should it be somebody within the organization? Should it be somebody outside of the organization? What are the internal threats that we might be facing? What is the last time we did a penetration test, for instance? What kind of issues might come up if you have some big transactions going on in the company, an M&A for instance, when you're trying to combine two different organizations? What get exposed? Once you get past the assessment, you start thinking about risk management. Who's in charge? What's the organizational structure? Is that a clear accountability for cyber security? Who are the best external agencies that can help us here? How should we be staffing? What's the right amount of resources that we should be putting into reinvestment answers?

Kenny: You even point out in the case, Target had thought about this, because you have an excerpt from a memo that was a risk assessment done in 2013, where many of these same issues were put on the table and I guess the message to board members who are listening to this podcast is: don't just sort of ask those questions and leave them unanswered and don't pay attention to them again, right?

Srinivasan: Absolutely. This is not a check-the-box exercise. Even though when you have a set of questions, the temptation might be to think of, "Once we ask the question, it's done." One question to ask is: how often do we ask these questions and how do we get comfortable that the company is responding to these? One of the things that comes up when I talk to a lot of cyber experts in a lot of companies is that who should be even checking on this? The information security are the people who execute it, should they also be the people who audit it? Should somebody else be auditing the information security infrastructure within the company? It's one, an issue of asking the right questions. It's an issue of who should be asking, an issue of how often should we be asking, and then what do we do based on the answers we get?

Kenny: Great questions. I guess the lesson for people like me, who shop at Target, is make sure you check your credit report frequently and your credit card statements, right?

Srinivasan: Absolutely. One of the things that also comes up with this is that there are so many externalities that are getting created because of something like this. If an organization fails, customers get affected. You could think about how to handle externalities like this. We handle it through regulation. In a way, this is as much as given there are so many state actors, it appears, that are getting involved in this. What is the role of the federal government in something like this? We don't leave an air space infiltration or a seaways infiltration to be dealt with individual companies, we take a response to the federal level. Is cyber warfare, if you can all it that, something that the federal government□certainly the federal government is very much aware of this and things that are going on, but it's also a question of how should companies be interacting at the federal level?

Kenny: I think I hear a B case coming, Suraj.

Srinivasan: There are lots of B cases in this. We read every week in newspapers about big things like this, which makes this issue extremely salient one for managers, for companies, for boards. We are also now using this case in our risk management programs for executives because it is a very important thing, where the threat is ever-present, but the ways of dealing with this, we are still learning how to do it.

Kenny: Thank you so much for joining us today.

Srinivasan: Thank you very much. My pleasure.

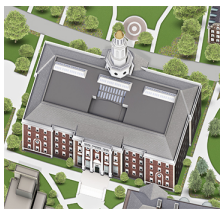
Kenny: You can find the "Cyber Breach at Target" case along with thousands of others in the HBS Case Collection at HPR.org. I'm Brian Kenny and you've been listening to *Cold Call*, the official podcast of Harvard Business School.

READ MORE

POST A COMMENT

In order to be published, comments must be on-topic and civil in tone, with no name calling or personal attacks. Your comment may be edited for clarity and length.

Write a comment



Harvard Business School Working Knowledge
Baker Library | Bloomberg Center
Soldiers Field
Boston, MA 02163
Fax: **1.617.495.6791**
Email: **Editor-in-Chief**

→ **Map & Directions**
→ **More Contact Information**

→ **All Social Media**