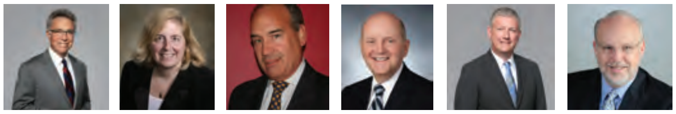
PROCEEDINGS OF THE 2014 EDI LEADERSHIP SUMMIT

CYBERCRIME:

ISSUES IN THE ERA OF BITCOIN & DATA BREACH

ADAPTED FROM A PANEL AT THE 2014 EDI LEADERSHIP SUMMIT IN FORT LAUDERDALE, FL

DISCUSSION BY:



MODERATOR:

ROBERT OWEN, PARTNER, SUTHERLAND ASBILL AND BRENNAN LLP

PANELISTS:

CHRISTINA AYIOTIS, ADJUNCT FACULTY, THE GEORGE WASHINGTON UNIVERSITY

PETER FOSTER, EXECUTIVE VICE PRESIDENT, WILLIS NORTH AMERICA

DAVID SHONKA, PRINCIPAL DEPUTY GENERAL COUNSEL, FEDERAL TRADE COMMISSION

MARK THIBODEAUX, COUNSEL, SUTHERLAND ASBILL AND BRENNAN LLP

DALE ZABRISKIE, PRINCIPAL TECHNOLOGIST, SYMANTEC

EDITED BY THE ELECTRONIC DISCOVERY INSTITUTE | AVAILABLE FOR DOWNLOAD AT WWW.EDISCOVERYINSTITUTE.ORG

LET'S TALK CYBERCRIME

The Heartbleed Bug is simply kindling an already well-fueled bonfire. An underground network of cyber-criminals is taking on some of the largest banks, governments and Fortune 500 organizations – and so far making it to the getaway car. Is the world under a new reign of digital theft by cyber-burglars? This panel, made up of our nation's leading experts on cybersecurity, will cover their current outlook on data breaches, data theft and cyber terror.

ROBERT OWEN: I'd like to begin by introducing our panelists. Dr. Z, this is Dale Zabriskie, a Principal Technologist from Symantec. Dale has been with *Symantec* for 14 years. He advises Symantec's clients worldwide on strategies for securing information. Dale is a *Certified Information Systems Security Professional* (CISSP) and is certified in cloud security knowledge. His clients include: *AT&T*, *Boeing*, *Fed-Ex*, *Ford Motors*, *IRS*, *IMF*, *State Farm*, China and Saudi Arabia. Dale's primary contribution to today's panel will be discussing his take on threat landscapes, cybercrime and breach response.

Next we have Peter Foster, the Executive Vice-President of *Willis North America*. Peter consults with clients on cyber-security in all industries. His focus is on combining insurance and preventative risk management to help Willis' clients worldwide. He has spoken on this topic in the United States, in Toronto, in London, in Hong Kong, in Rotterdam, Tokyo, Johannesburg. His primary contribution is going to be on breach preparedness, corporate governance and insuring against cyber-risk.

Christina Ayiotis, an adjunct faculty member at *George Washington University*, in Washington, DC, is a long-time friend and supporter of EDI. She has been instructing on subjects including cybersecurity, privacy, big data, social media, records information management and eDiscovery for 6 years. Christina is a true expert in this area and a real asset to all of us here at EDI.

Last, I would like to introduce you to Mark Thibodeaux, counsel at *Sutherland, Asbill and Brennan*. Mark is a commercial litigator in our Houston, TX office. He counsels clients on all types of discovery, one of which included the owner of a drilling rig in the famous gulf oil spill. He has really been "in the eye of the hurricane", if you will, in these matters. Mark began his professional career as an auditor at a Big 4 firm, where he worked for about 8 years. Mark was once hired by Enron to be a *white hat hacker* into their system. This raises a question - Mark, how did you learn to hack?

MARK THIBODEAUX: Some questions should remain unanswered.

ROBERT OWEN: After successfully fulfilling his duties in that position, Mark became Chief Information Technology Officer at *Enron* and worked there during the bankruptcy. Mark is also a *Certified Information Privacy Professional*. We are very happy to have him.

It may be a coincidence, but, as soon as I became involved in chairing this panel, it seemed like I was seeing evidence of hacks every single day. Some of the big names: *Jimmy Johns*, *Healthcare.gov*, *Home Depot* and *Apple iCloud* in September. *JP Morgan Chase* and *Dairy Queen* in August. The USIS... (this happens to be the organization that performed the background check on Edward Snowden. They did not get their contract renewed and now about 2,000 people are out of work.) *UPS*, *Albertsons*, *REI*, *The Wall Street Journal*, *Total Bank*, *Bank of the West*, *Good Will Industries*, *C-Net*, *Boeing* and *K-Mart* to name a few others. This is not something that is a latent, sometime risk. The lesson for all of us to take back to our clients and our companies is:

"YOU NEED TO PREPARE FOR CYBERCRIME NOW BECAUSE YOU ARE A TARGET. YOU WILL BE HACKED."

Our panelists will explain that no matter how good your systems are, there is most likely going to be a successful incursion at some point. The traditional view of security is a castle with a moat around it. Was it ever really this simple? Maybe at one time, but, it certainly is not now. We have got laptops, tablets, smart phones and portable media. All of these apps on your screen. There are so many ways for the bad guys - and maybe the bored teenagers - to hack into these systems to steal your information. Whether it's an opportunistic download of information off of a laptop or whether it's something that was concerted and deliberate, there are a million ways to do this. This is a very real problem.

IDENTIFYING THE LOCATION OF CYBER-THREATS

DALE ZABRISKIE: I will begin with a view of Symantec's Security Operations Centers. There are three of these around the globe in London, Washington, D.C. and Sydney, Australia. This is a 24/7 operation where we oversee activity on the networks of the world. There are approximately 150,000,000 installations of our technology throughout the world. We have the ability to view 30% of the world's SMTP e-mail. It is a remarkable set of network sensors, "honey pots" and different pieces of technology. Through this last year we were able to block about 6.6 billion attacks a day.

ROBERT OWEN: How many?

DALE ZABRISKIE: 6.6 billion.

ROBERT OWEN: Billion?

DALE ZABRISKIE: That's correct. It's extremely active, as you can see. It's extremely secure. This is the knowledge behind the technology. Technology is important. Everything that you need to protect your physical assets is important. But, you have to have context and relativity behind what's really happening. You need to know where threats are going to come from. For example, 4 years ago, there was an attack focused on centrifuges in Iran. It was our systems that identified where that attack was coming from.
It was two command and control servers, one in Denmark

and one in Malaysia, which were pumping out this malware. Those ISPs - they were service providers - they had no idea. We were able to locate the attack and identify what they were attacking. This is the key to what we do for companies worldwide: we provide the knowledge behind the technology.

Peter Foster: By the way, it's rumored that particular piece of malware first got onto the systems in Iran via the networks.

Dale Zabriskie: The networks…yes. Be careful with that thumb drive you have on your table. The networks at that facility were air-gapped. Meaning that there is no physical wire or wireless connection to the internet from that network where those centrifuges are contained. There is an air gap between the internet and that. It jumped the air gap probably through a thumb drive or a portable drive, and it's the first real malware that we saw that physically controlled something. It caused the centrifuges to spin erratically and to make it look like everything was okay. It was extremely sophisticated.

"THAT WAS A TIPPING POINT FOR SOPHISTICATED MALWARE IN THE WORLD."

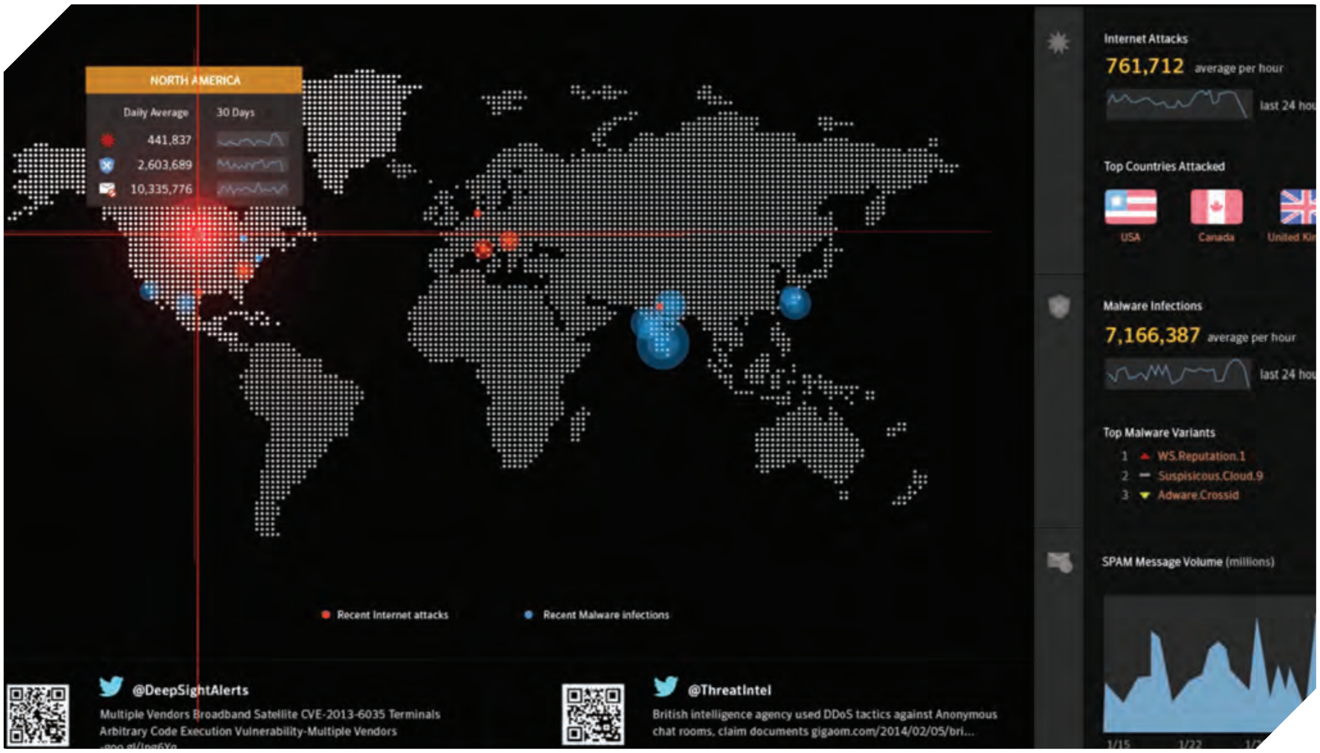
Christina Ayiotis: We believe it was the first offensive cyber warfare operation.

Robert Owen: So, do we know who was behind it? Can we say?

Dale Zabriskie: The word on the street is that it was a joint effort between the United States and Israel. There is nothing specific that has articulated that yet, but, there is enough circumstantial evidence. This attack is an example that would require a very large team of people, about 6 months and a lot of money behind it. The other money that's out there is involved in cybercrime. When you see organized crime being extremely involved with many countries to produce malware, whether it's China, Russia or others, they are very well funded. These are the things we are starting to see that are extremely difficult to deal with.

The next example I'd like to discuss is called *Deep Sight*. It is a threat monitor. It's a view into activity.

"THE AVERAGE NUMBER OF INTERNET ATTACKS IN THE UNITED STATES IS 761,000 ATTACKS PER HOUR."



@DeepSightAlerts
Multiple Vendors Broadband Satellite CVE-2013-6035 Terminals Arbitrary Code Execution Vulnerability-Multiple Vendors

@ThreatIntel
British intelligence agency used DDoS tactics against Anonymous chat rooms, claim documents gigaom.com/2014/02/05/bri...

That's just in the United States! On average, there are 7 billion malware infections per hour. It's just incredible. The evolution of the threats has gone from the things that are visible and noisy in the sense that everybody's getting hit. Do you know anybody who is still waiting for their 10 million dollars from Nigeria, anybody? Yeah. We are all waiting, right? Why do we keep getting those e-mails? Well, because they work.

The other side of it is that it's targeted. This is the evolution to where the threats are now becoming so specific. You are going to get an e-mail from someone that said "I saw you at that EDI Leadership Summit, here's a link to something that you might like to see." They know you were attending because you put it on a site like Facebook or Linked-In and, they would do a profile.

> "THESE TYPES OF FOCUSED, TARGETED ATTACKS THROUGH E-MAIL ARE ON THE RISE. WE HAVE SEEN A 91 PERCENT INCREASE IN TARGETED ATTACKS OVER A 12 MONTH PERIOD."

WHO ARE THE HACKERS AND WHAT ARE THEIR INTENTIONS?

CHRISTINA AYIOTIS: I think it's important to think through exactly what the hackers' intentions might be. While you, of course, have criminals who want to very quickly steal something and profit from it, you also have people who want to disrupt. They are not actually getting into a system but they are making it such that it is a distributed denial of a service (DDOS) attack. They are attacking so much that you are not actually able to give a service.

Another thing that has the government and a lot of companies even more worried is the ability to get in and to degrade or change information in such a way that you can't detect it. As time goes on, companies like Dale's are going to come out with the ability to make sure that they are able to track that because that's even more insidious.

TODAY'S THREATS:

CRIME
HACTIVISM
ESPIONAGE
WAR

DALE ZABRISKIE: Forensics is a difficult thing in a cyber-space war. This is an excellent point. Take a guess at what the number one country of origination of denial of service attacks is? And, I will give you a hint. It's not the U.S. The U.S. is number two. I will give you another hint. It's not China. It's not Russia and it's not Iran. It's India. The technology is evolving, and people are evolving. Now we see this shift of where these threats are originating from. For the first time, India is taking the top spot of distributed denial of service attacks. The other thing about these attacks is that they are often done to force you to look in one space while the bad guys are going through your pockets. They will bring something down to get attention while they go over and quietly do what they really want to do.

MARK THIBODEAUX: You say, the U.S. is number two on that list but there's a lot of reason to suspect that that's because people's home computers and the computers at work have been hacked into and are being used to launch secondary attacks that actually originate somewhere else?

DALE ZABRISKIE: Yes. Exactly.

PETER FOSTER: The National Coordinator for Security, Infrastructure Protection and Counter-terrorism for the United States, Richard Clark, defined how they are specifying who the hackers are. They are criminals, activists like *Anonymous* or *Greenpeace*, espionage, perhaps with the Chinese and in some cases other friendly governments like France or Israel.

Mark Thibodeaux: One of my clients is a children's hospital. They were attacked by a strand of *Anonymous* - the creator of *Anonymous* said that he was not involved in this because he did not want to punish a children's hospital because of their choice. It was all over a decision about releasing information about a child and actually holding a child against their parent's will. The fact is that the *Anonymous* strand actually attacked the children's hospital, shutting down a number of their servers and causing them not be able to provide treatment to patients. That's an effective way of shutting down a business which of course created additional problems down the line.

Robert Owen: What is *Anonymous*? We have all heard of it, but can you all tell me what it is?

Dale Zabriskie: They are a loosely organized group of people.

Mark Thibodeaux: This loosely organized group of people share a common bond, a common socio-political bent. They think everything should be open, everything should be free and accessible. South Carolina had a major data breach with 70 agencies and *Anonymous* was behind it. These are the kinds of cause and effect things that are happening.

Robert Owen: So, what happened to the bored teenagers?

Dale Zabriskie: They grew up.

Peter Foster: There are still a lot of very clever teenagers out there that do hacking merely for the thrill of doing it and in some cases in competition with other youngsters that are doing the same sorts of things. I actually had a client whose systems were broken into. They first found out that they had been broken into from the victim's letter that the Department of Justice sent to them. They did not detect the attack on their own. They ultimately found out that the guys who had broken into their systems had done so to prove that they were better than another hacking group.

Cyber-Espionage

Christina Ayiotis: I would like to highlight the issue of cyber-espionage - for a corporate audience - it is very important to think through your current strategy to protect your intellectual property and your information assets. That's the real threat. The cyber-terrorism threat gets a lot of attention and of course something could happen. But, the real threat to our national security is the economic threat and the ability for folks to be able to take our intellectual property and use it in other places, depriving the U.S. companies of the ability to make money.

How Are the Hackers Getting In?

Peter Foster: Hackers gain access in so many different ways, either through negligence of your employees - whether that is lack of protection of their own passwords - or the security not being installed effectively. The hackers are bright today. They are figuring out different ways to get in other than what you have protected against. You are all hearing about the retail issue and it is the point of sales terminals that are lax in security right now. Even if they do have security, there's no pin and chip technology here in the U.S. in credit cards. Therefore, you have an exposure there. Many retail companies are just dealing with alerts as they hit the network. The different malware is already present on their systems. There are so many attacks, as Dale alluded to earlier, organizations don't know what to prioritize right now. That was the big miss on *Target*: prioritizing that critical issue that's on your network today.

Specifically Targeted Attacks

- *Phishing*
- *Spear phishing/Longlining/Whaling*
- *Water-holing*

Advanced Persistent Threats (APT)

- *Hackers lying in wait*
- *Selling time on your computers*

The Enemy Is Among Us

- *Employees and contractors already have access*
- *They do not need malicious intent to be a problem*

LESSONS FROM A RETIRED HACKER

ROBERT OWEN: Mark, you were a hacker. Is there a place on the internet where we can go and learn how to do this?

MARK THIBODEAUX: Yes, just start with *Google*. You can find sites where you can download tools. You don't actually have to know anything, you just sort of point and click and the hacking tools available out there will surface.

One of the points about how hackers are getting in relates to that picture of the castle with the moat around it. Many people still think, “We have a corporate network and we have got a firewall facing the internet. Anything inside the firewall is automatically more secure or safer than things that are facing the internet; my web servers and things.” When I first started at *Enron*, one of the first systems I tested was a platform called *Enron Online*. At the time it was the largest online commodity trading platform in the world. It was doing nominally, $1,000,000,000,000 worth of transactions a week. I broke into it in about 5 minutes.

It really did not have very good security. When I told those responsible for running the system how I had gotten in, they said “Well, you cheated. You didn’t get in through the internet. You didn’t break in through our firewall.” I was like, “No. I broke in from the inside. I had an account on your network and I broke in through the network. By the way, you have offices in 38 countries. You have 40,000 employees world-wide. You have contractors coming in and janitors and everybody else. You don't know who’s inside the firewall or what they are doing.”

"YOU HAVE GOT TO HAVE SECURITY JUST AS GOOD WITHIN THE FIREWALL AS YOU DO FACING THE INTERNET."

DETECTING AN ATTACK

ROBERT OWEN: I have read that often, successful hacking can exist and persist for 200-300 days before the company even notices. How does that come to light? How do we know we are being hacked?

DALE ZABRISKIE: The average number of days that a piece of malware sits on a system before it is detected has risen to 243. *Target* is a good example. This is what I call the burnt marshmallow syndrome. You remember sticks and marshmallows and campfires, right? A burnt marshmallow is very strong and crispy on the outside but is extremely fluid on the inside. It moves all over the place and that's the way a lot of these environments are. If you are not directly involved in IT, you are so busy worried about other things that you tend to lose focus on the processes and policies and the activity on the inside.

A lot of the data breaches have also been the result of, for lack of a better term, “ignorant people.” Employees who are just trying to get their job done and they just do something that's either part of the process because it’s always been that way or they are just really lax that day and they do something that's against the process.

All companies and organizations need to do is take a harder look at the activity on the inside because that's when you start to see anomalies. You think about one of the first poster children for data breaches: *TJ Maxx* (about 8 years ago). That malware sat there for months just siphoning off activity. The movement of information is such an indicator of its activity. It goes back to the point made earlier about intellectual property.

"WE NEED TO SEE INFORMATION MORE AS TANGIBLE ASSETS ON BALANCE SHEETS. BECAUSE INFORMATION IS TANGIBLE AND IT WILL AFFECT THE BOTTOM LINE."

There are different types of tools and technology that can detect activity. The security spend is a tough sell often because until something happens, nobody wants to buy the insurance. The problem is very real.

"I HAVE ALWAYS FOUND THAT PLANS ARE USELESS, BUT PLANNING IS INDISPENSABLE."

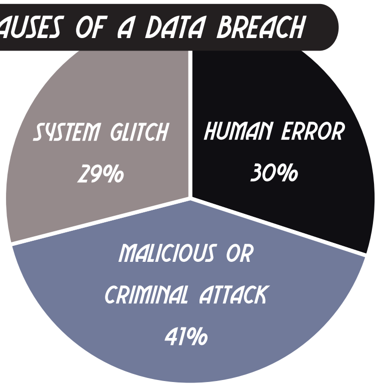
- PRESIDENT DWIGHT D. EISENHOWER

BREACH RESPONSE AND REMEDIATION COSTS

ROBERT OWEN: Peter, your career involves marrying insurance coverage and risk management and you have been involved with some of the biggest hacks of recent times. What are the costs of breach response and remediation just in general categories?

PETER FOSTER: I think there are some fallacies out there that a breach is going to cost you $200 to $500 per record. I am not seeing that. I am seeing a cost - if it's a smaller breach of 100-1000 records - of $18 to $20 per record. But, on some of these bigger breaches the loss is below $5 per record. Everything is weighed into that: the litigation costs, the settlements with credit card companies and the regulatory fines that are assessed against you by the State's Attorney General. If it is healthcare information, it could be HIPAA fines. All those costs, when you weigh in that it affected about 45 million people, it really comes down to a few dollars. The problem is that the class action attorneys are out there and they are only looking for a few dollars per record because they can build a significant loss out of just that.

ROOT CAUSES OF A DATA BREACH



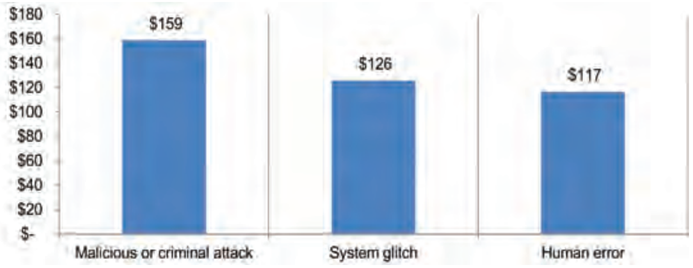
DUE DILIGENCE: TESTING EVERYONE FROM THIRD PARTY VENDORS TO YOUR OWN BOARD OF DIRECTORS

CHRISTINA AYIOTIS: From a corporate perspective, there is the issue of third party vendors and the risk that you have when you are outsourcing your business functions, your data or even your customer's data. It is sitting outside of your environment without full visibility all the time. There is a process by which in-house lawyers need to work with their supply chain colleagues and others to ensure that at the front end, the proper diligence is done. The protections and controls need to be built into the contract. And they need to be regularly audited to know what is happening because the threat comes from third parties. This is true for any vendor, for anything, whether it's HVAC or one of your service providers or even your most trusted advisors. Your accountants and attorneys have access to your most sensitive information and you have to put them through the same rigorous due diligence.

DALE ZABRISKIE: Excellent point. It's interesting when you look at *Target*. It has become a noun, a verb and an adjective all of the sudden. *Target* was hit by a third party, an HVAC contractor. Number one, how much did you think an HVAC contractor was connected to credit cards at *Target*? You don't make that association. Their systems allowed that association. Now, shame on *Target*, but, not everyone thinks of these things.

The Hartley, the Bash and this thing that came out in October called Poodle. They are all exploits of technology that have been around for a long time. The Bash thug has been sitting on servers and systems for 22 years. The bad guy actors are out there thinking about things that we have forgotten about. It's part of that inside of the marshmallow. There is an interesting trend happening right now focused on these little things that have been operating across the systems of the world that we have forgotten about. They are however exploitable in big ways and cause great havoc.

PER CAPITA COST FOR EACH ROOT CAUSE



Christina Ayiotis: They get in through processes that allow third party vendors access to your network. The hard part is putting someone through the rigorous process of ensuring and auditing that they only do what they are allowed to do.

Peter Foster: You can have the most robust security policies in the world at your company and if everything at the company ends up becoming an exception to those policies, you probably don't have as good security as you think. I see that all the time. A CEO calls the CIO and says "I'm tired of having to change my password every 2 months. It's driving me crazy and I can never remember it. Can I get an exception?" Sure. You are the CEO and I'm going to say "No?"

Christina Ayiotis: Or the Board. That's one thing that you want to make sure to lock down because they have the most sensitive information.

Breach Costs Are Increasing

Average cost of data breach increasing

COST PER RECORD IN 2013 (U.S.): $188
COST PER RECORD IN 2014 (U.S.): $201
COST PER RECORD IN 2013 (WORLD): $136
COST PER RECORD IN 2014 (WORLD): $145

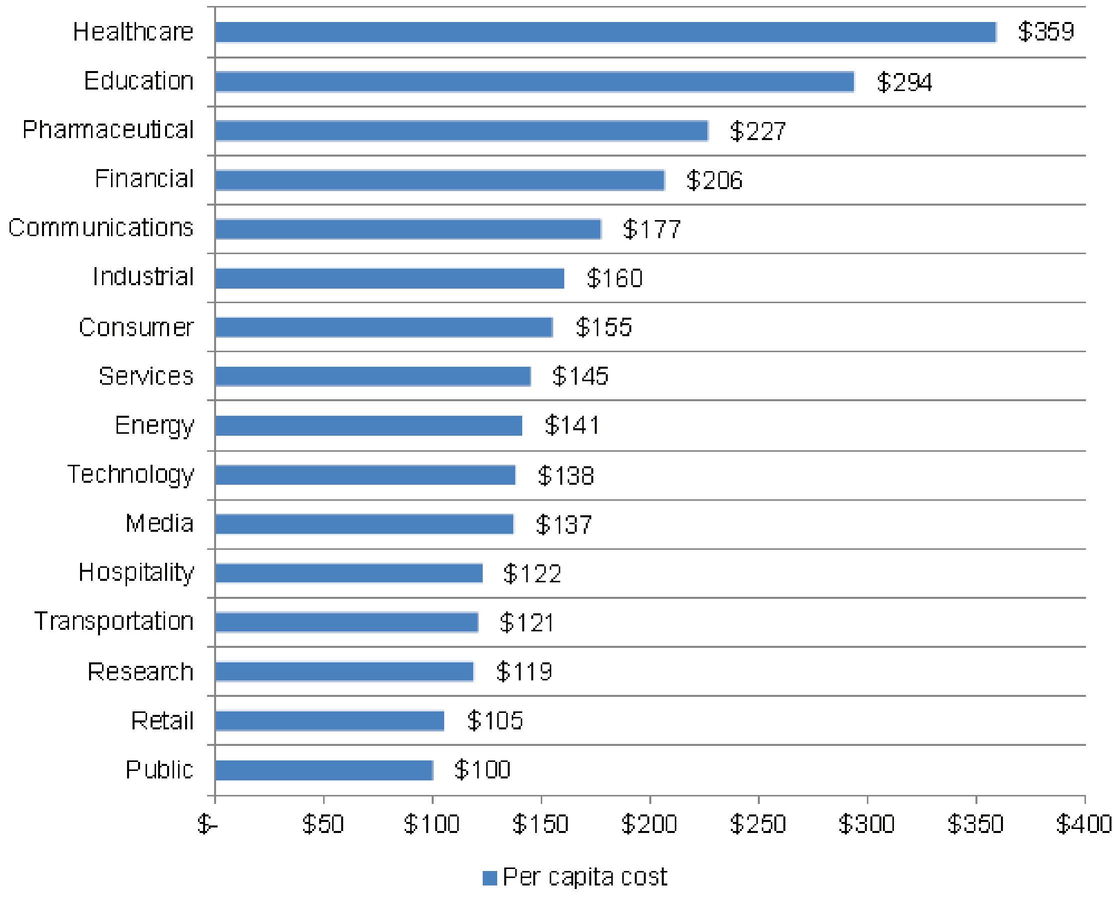
Average size of data breach

U.S.: 29,087 RECORDS

Average spent on notification

U.S.: $509,237

Breach Costs by Industry



THE SHIFT TOWARD DIGITAL CURRENCY: WHAT IS CRYPTO-CURRENCY?

DALE ZABRISKIE: We are taking a shift towards digital currency. The shift has been going on for quite a while. Now we are seeing the use of cryptography to create a currency that is not regulated by any financial organization. It's an open-sourced, crowd source experience.

Bitcoin, is the most well-known, but, there are probably 100 different crypto-currencies out there today. Most of them are derivatives of Bitcoin (which goes back to about 2009). There is essentially an open system by which you have mining of Bitcoins and you trade them. Many companies are accepting Bitcoins now, although, the problem is that they are very volatile. There was a group in Japan that went bankrupt with $473 million worth of Bitcoins. The value of one Bitcoin went from approx. $1,100 to $300 in a matter of minutes. Due to our global connectivity, this is something that is on its way and is going to be organized.

I think that the whole aspect of our lives and the internet is trust, right? We trust these algorithms and the cryptography to protect us. There are in fact, a bunch of people who want us to succeed, but there are just as many people out there trying to break it down and trying to get through it. It's an evolution of technology and society that brings this together. Bitcoin is pretty common place now; you can buy a lot of stuff with Bitcoins.

THE "DARK NET"

MARK THIBODEAUX: The *Dark Net* is an encrypted branch of the internet where transactions and discussions can take place in relative anonymity as long as the cryptography holds up. It is being used by organizations ranging from the activists in Hong Kong to the intelligence community. There are all kinds of good purposes behind the *Dark Net* like anonymous free speech. But, then there are those things you hear news stories about, things like a website called " *The Silk Road, Anonymous Market*," which is run in the *Dark Net*. *The Silk Road* was selling everything from illegal arms to illegal medications to hit contracts to whatever you can think of. You might say that free speech has its costs.

ROBERT OWEN: How does it work?

MARK THIBODEAUX: Cryptography - you basically install software on your PC, usually it's done with a particular piece of software called *the onion router* or *Tor*. It encrypts all of your communication and everybody who's participating in that type of encrypted communication. The encryption keeps answering, "No", until it finds that network that agrees to anonymize and pass on your communications. It goes to another mode and another until it comes out somewhere in which you can't trace it anymore.

REGULATION AND THE FTC

ROBERT OWEN: At this point I would like to introduce, David Shonka, Principal Deputy General Counsel from the *Federal Trade Commissoin (FTC)*. David, who is policing the internet from the regulatory point of view? What statutes does the FTC use when policing cybersecurity at companies with at least one foot within American jurisdiction?

DAVID SHONKA: There's really a hodge-podge of statutes and regulations that govern an awful lot of what we do. The financial industry is subject to one set and healthcare, we have all heard of HIPAA, is subject to another. There are a variety of sectorial laws that touch the area. What remains after that is everything else that's not separately regulated. The FTC is a small agency with a very broad jurisdiction. It basically has authority over all for-profit operations that are not regulated by someone else, which means most of the economy. It comes down to the FTC Act and what we can call,

"U-DAPS: UNFAIR AND DECEPTIVE ACTS OF PRACTICES. SECTION 5 PROHIBITS UNFAIR AND DECEPTIVE ACTS OR PRACTICES THAT ARE AFFECTING COMMERCE. THAT IS THE RANGE OF THE FTC'S AUTHORITY."

So, then, the question is, *what is deceptive*? The answer has been pretty well established by now. The FTC has been doing this for 100 years. Deception can be expressed. It can be implied. It can be a direct statement or it can be a material omission. If people are giving information, false or deceptive information and consumers are relying on that to their detriment then you have a violation of the *Deceptive Act of Practices* section of the FTC Act.

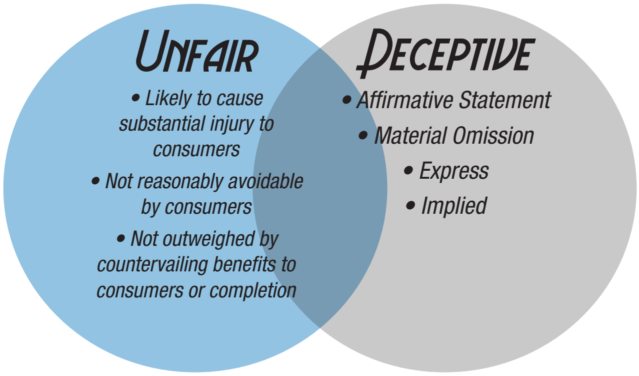
Then, there is unfairness. Section 5N of the FTC Act defines unfair acts or practices as any act or practice that is likely to cause substantial injury to consumers that they (consumers) cannot reasonably avoid and that has no off-setting counter benefit. It's a 3-part test.

Can the consumers, by taking reasonable steps, avoid being injured by the practice or act in question? Even if they can't avoid it, is there some off-setting benefit, some countervailing benefit that outweighs that? The idea is simply the overlapping circles of the old Venn diagram. An act can be deceptive without being unfair; an act can be unfair without being deceptive. On the other hand, some acts or practices are both deceptive and unfair. The FTC gets into the picture when we are looking at conduct that is either deceptive or unfair. That is going to be a matter of concern for us.

CHRISTINA AYIOTIS: I'd like to give an example, if you have a third party vendor managing personal information from the EU, you can avail yourself of the *Safe Harbor Certification* that the Department of Commerce provides. It's a self-certifying process. However, if you say you are *Safe Harbor Certified* and you actually are not, the FTC can come in and enforce that. There are companies that have said they are doing it but they are not really doing it. If you are in-house counsel and one of the vendors that you are looking at says, "Oh, yeah, we are *Safe Harbor Certified*. No problem." Please, people, just don't take their word for it! Do your due diligence because you don't want to be in a position where you relied on someone else.

DAVID SHONKA: Recently in this particular area, the FTC has announced an enforcement initiative and is looking at and paying attention to companies that claim they are *Safe Harbor Certified* and are not. That's a particular brand of deception that would be interesting to the FTC.

FTC CYBERSECURITY ENFORCEMENT


UNFAIR
• Likely to cause substantial injury to consumers
• Not reasonably avoidable by consumers
• Not outweighed by countervailing benefits to consumers or completion
DECEPTIVE
• Affirmative Statement
• Material Omission
• Express
• Implied

Robert Owen: David, talk to us about the way in which the FTC has settled the charges that it has brought over the last few years. One of the requirements of the Facebook consent order, I believe, was an audit or a check of their systems for the next 20 years. Some people look at that and say "Wow! That's a long time, and isn't the world going to change a whole lot in 20 years?" How did the FTC get to that place and how does it intend to administer those consent orders over the next 20 years?

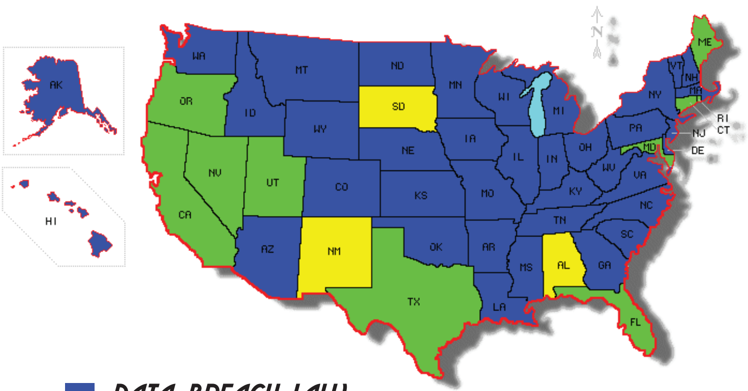
David Shonka: The short answer on how we intend to administer is there are reporting requirements. Of course we have a compliance division; enforcement actually is what it is called on our consumer protection site. Our enforcement division takes the reports, looks at them and depending on resources and what it finds, may or may not pursue restitution or civil penalties for violating an order.

Everybody thinks that if there's a data breach, the FTC is going to get the company that has suffered the breach. That's not really what happens. For us, the fact of a breach is only one thing that may trigger an investigation. There may be other things as well. If we find that a breach has occurred, it's going to be a matter of some interest. We may very well come at a company and ask them for information concerning their security systems. Depending on what we find, we may or may not be concerned.

I point you to the castle with the moat around it as an example. If somebody has a castle with a moat around it and somebody else tunnels under the moat and comes up in the middle, then they've gotten through all of the security defenses despite state of the art - and it's not even state of the art defense. If somebody manages to get through in spite of the defenses, the FTC is just going to say "Sorry." That's probably going to be the end of the inquiry. The standard is not perfect but reasonable and appropriate to the circumstances.

"THE LEVEL OF SECURITY PRACTICES THAT A SMALL COMPANY WITH NO PARTICULARLY SENSITIVE DATA OR CONSUMER INFORMATION ARE GOING TO BE HELD TO ARE MUCH DIFFERENT STANDARDS THAN FOR AN ORGANIZATION THAT DEALS WITH PERSONAL CUSTOMERS' ACCOUNTS, MEDICAL AND FINANCIAL INFORMATION."

You know some people like to say, "Well, gee, if we are a small company shouldn't we be let off the hook on this sort of a requirement?" My response to that argument is, if you want to handle uranium don't tell me you can't afford a container to put it in. Those sorts of things can cause immediate and substantial harm. The fact is ultimately you have to have some defenses suitable for what you do.



🟦 DATA BREACH LAW
🟩 DATA SECURITY LAW
🟨 NO DATA LAW

RIGOROUS STATE LAWS GOVERNING DATA SECURITY

Peter Foster: There are now approximately 48 state laws governing consumer protection of personal identifiable information. Legal compliance folks are looking at Massachusetts law as the leading law on where we should be going. So, if I have operations or, better yet, customers or employees in a number of different states throughout the U.S., I'm looking at Massachusetts law right now. Massachusetts has certain requirements about access controls, data classification, vendor management and holding vendors to the law.

Mark Thibodeaux: Although, again, showing that this is a very volatile area, there are a lot of people saying that Florida has recently passed laws now which leapfrog Massachusetts as the highest standard in states on data security issues.

Christina Ayiotis: If you map the requirements for the Massachusetts law against other standards like the ISO Standard 27001, you would see a lot of the same components. It's really about being proactive to protect. That's actually what the rest of the world requires on the front end. You have to put controls in place and not just worry about what happens after something goes wrong.

THE NIST FRAMEWORK

Robert Owen: We have read about the NIST, National Institute of Standards and Technology, framework. Can somebody explain why our audience should care about it?

Christina Ayiotis: The Executive Branch put an executive order in place - designated the Department of Commerce's National Institute of Standards and Technology - that looks at existing standards to pull together a framework that will take a risk management approach. It's not that they reinvented anything. They pulled controls that already existed together and put it into a format that's not very long. It set up an expectation that if you are in a particular industry, you need to abide by whatever your industry specific regulation is.

Dale Zabriskie: The key about the NIST framework is that it is consumable, digestible at 20 controls. There are things like COBIT, Control Objectives for Information and Related IT. These frameworks are all very good to help focus in on what organizations need to do. If you are in finance or in healthcare, there are specific regulations, but, outside of that, that's where a lot of the threats are still being propagated.

This is just a framework, an idea. It is just a way to start looking at things. We still require process and policy in the back-end to ensure that these things are happening. The idea of compliance means that there are regulations, therefore, there is a policy. If there are regulations, then there are controls, and therefore, governance. The governance aspect has to look back and remediate. Auditors really want to see proof of due care.

> "AN AUDITOR'S DESIGN SHOULD SHOW ME WHAT I DON'T KNOW AND WHERE MY HOLES ARE SO I CAN PLACE THE RESOURCES THERE TO ADDRESS THEM."

You have got to use the process of governance and remediation in order to really succeed regardless of what you are trying to comply with.

National Institute of Standards and Technology (NIST) Cybersecurity Framework

DETER
identify risks

DETECT
unauthorized access and activity

PROTECT
safeguards for systems, vendors

RESPOND
response plan, communications, mitigation

RECOVER
restore capabilities

Mark Thibodeau:

> "IT SECURITY HAS NEVER REALLY JUST BEEN AN IT PROBLEM AND IT'S CERTAINLY NOT SO TODAY."

There are large aspects of the NIST framework that help you at least obtain a common language. When lawyers are talking to IT or executive management, they have a common way of talking about cybersecurity. Your IT guys can't tell you what your most critical data is. That's a business decision.

David Shonka: Let's revert back to this idea of the audit and why it's so important. The audit provision is performed by an outside, independent auditor. Somebody who does not have an interest in trying to protect or cover up anything. Somebody who can come in and take an objective look at the system, the process that the company has in place and then write a report on it. Based on that objective, independent evaluation, the company is then expected to make any adjustments in the system going forward. That process is critical. If the FTC requires an independent auditor to look at something for 20 years, it simply means that companies need to get into a habit. It has to be what they do all the time, routinely. It has to become part of the system.

THE GOVERNMENT AND BREACH DETECTION

CHRISTINA AVIOTIS: I'd like to go back to the question of how people find out that something has happened. Very often the government is coming to tell you. Three major pieces of the government that are focused on this are the Department of Homeland Security, the DOJ/FBI and the NSA, which is part of the Department of Defense. It depends on what the situation is in terms of whether it's a national security issue and whether it's a nation state actor verses a criminal actor, etc. There has to be a mind shift regarding the way companies think about how they are going to interact with the government and have a proactive open relationship with communication. The FBI has a program set up, called InfraGard. You join it, you get information. You don't have to pay for it. The Department of Homeland Security, as a result of the NIST framework, has set up industry groups to support people. They will give you clearance for a day to get briefed, so your business people can acquire information.

DAVID SHONKA: In the South, people often learn of problems because the FBI or somebody tells them. The fact is that's not the only way. I had indicated that a breach is one thing that can cause an investigation by the FTC but there are other things. Sometimes we see complaints by consumers or by even disgruntled employees who will say to us, this company really has bad security practices. If the information we get is

creditable, we may pursue it. And, if we pursue it and open an inquiry and we see things like lack of training, lack of any program, written program for security, lack of inability to detect intrusion or anything else, then we are going to be interested.

Out of the 50 some cases that we have seen, I will argue that in each and every one of them, what we found were widespread and systematic failures to maintain sound security practices in the company. It wasn't any one thing. It wasn't because somebody lost the computer. It wasn't because somebody had a bad or a weak password. It's because there were practices in the company that persisted for a long period of time and they were widespread and systemic.

ROBERT OWEN: I was really interested to hear that the government has a database that tracks consumer complaints.

DAVID SHONKA: That is one tool we have. We have what we call a Consumer Sentinel Database, which is simply a hotline or an e-mail. People can call or write in and we will record their complaints and put them into a database. That has several different data fields about companies involved and the nature of the complaint. That goes online. It is available to something like, at last count, I think, it's 10,000 and counting law enforcement agencies, Federal and State governments, local governments and even the Canadian authorities. All this is information is raw material information. It is shared with other agencies and they can look at it and mine the data to find out sources of complaints, subjects of complaints, topics and so on. That can sometimes inform areas where we want to develop some resources and do some inquiries.

PUBLIC RELATIONS AND THE FBI

DALE ZABRISKIE:

"THE FBI WILL RUN TO HELP YOU DETERMINE WHAT YOU NEED TO DO IN CASE OF A DATA BREACH."

You have to consider this like your business continuity plan. We all have plans that if the systems go down, we have fail-over. We are going to back up or we are going to do this or that. The same thing has to apply to data breaches. We have got to have a plan. What if? When do I contact the FBI? Call them today and have them come in. They will gladly sit down with you and explain: here's the procedure and here are all the ifs, ands or buts. From a PR perspective, what are you going to do? How are you going to communicate this? There are lots of firms and organizations that are there to help with this process but you have to develop your plan ahead of time. The reactionary thing is killing a lot of folks. It's the whole reputation of your company. Get the FBI. Get them involved up front so that you know what to do when this something occurs both from a forensics and from a public relation approach.

PETER FOSTER: There's no one who has experienced more attacks than the FBI. One of my clients had the FBI involved immediately. They basically walled off a certain area within the network. They knew the hacker was coming back and they took the data and they marked it just like you would mark money. When the hacker came in and took the data they could follow the data and track down the criminals.

PREPAREDNESS

TABLETOP EXERCISES

- TESTING HELPS YOU IDENTIFY WHAT PARTS OF THE PLAN WORK, AND WHAT PARTS NEED WORK
- HELPS PARTICIPANTS STAY ENGAGED AND MITIGATE AGAINST HUMAN REACTION (I.E., PANIC) IN THE EVENT OF A REAL INCIDENT
- PRACTICE WITH A VARIETY OF SCENARIOS
- EXERCISES SHOULD INVOLVE ALL MEMBERS OF THE TEAM, INCLUDING EXECUTIVE LEADERSHIP

EMPLOYEE TRAINING

- MOBILE DEVICE POLICIES
- DON'T CLICK ON THAT LINK
- WHO TO NOTIFY AND WHEN
- WHO TO CONTACT WITH QUESTIONS

PREPARING FOR A DATA BREACH

ROBERT OWEN: Peter, how do you prepare your clients for data breaches? What are the steps? What do clients do and how do you help?

PETER FOSTER: How many of you in the audience have an incident response plan in place for a data breach and how many of you have had it tested?

ROBERT OWEN: About 10.

DAVID SHONKA: The key thing is to have a plan in place and have the stakeholders involved. Make sure that there is more than one individual who will make a decision about when to notify consumers or employees that their information was accessed. Then you really have to test that plan, having many of the stakeholders involved in that test. Run a table top exercise where you are really running through an actual breach. What would you do? How would you do it? You throw in different wrinkles as you move through it. This is one of the most important things:

"YOU DON'T WANT YOUR ACTUAL INCIDENT TO BE THE FIRST TIME YOU HAVE EVER RUN THROUGH YOUR INCIDENT RESPONSE PLAN."

Robert Owen: It's not just an IT problem. If somebody from your legal department is not being involved in those exercises, you are doing it wrong.

Peter Foster: It's legal. It's HR. Employee breaches are huge to marketing. It's everybody. You have to look beyond IT. This is not an IT or an IT security issue alone. Certainly, putting policy in place is a tremendous part of the response to a breach, the prevention of a breach. If you are not responding, you heard today of different regulatory bodies that will get involved. If you are across a number of different states, if you are in healthcare, etc., you have to look at all those laws to determine what you should be doing from a compliance standpoint. Your response could be both looking at states, looking at whether or not in healthcare, you have to give notice to certain individuals. All of that weighs in. Then you want to determine whether or not forensics should be involved. Should you go outside? If you are a publicly held company, I always recommend that you go outside to a forensics' engineer because you want to be able to tell the street and your shareholders that you are not just having your folks internally look at the incident. You want to say that you have hired a strong firm in order to do the forensic testing on this to make sure that you have captured everything that could be the problem.

Dale Zabriskie:
I always like to tell people that you may have brilliant IT staff who are very good technically and very good at doing security related things, however they are almost never trained investigators and they don't know the process or procedures. They don't know about evidence preservation. You need to have somebody who knows that skill set doing your investigation.

Data Breach and the Ligitation Landscape

Mark Thibodeau: Broadly, data breaches happen and the plaintiffs' lawyers immediately descend, trying to file class actions because there's usually hundreds of thousands, if not millions, of individuals affected. Largely, the class actions have been very ineffective. Courts have been throwing them out for failure to say that there is common harm amongst the class members. When somebody's credit card information is stolen that's not an automatic harm.

> "Having to spend 30 minutes on the phone getting the credit card replaced has not been seen by the courts to be a significant enough harm to justify a class action proceeding."

As attorneys though, hope springs eternal; they have used at least 86 different causes of actions in the class actions that have already been filed. I am sure they will come up with another 86 in the next couple of years.

There have been a couple of cases I want to mention that indicate that there may be hope for plaintiff attorneys. The 9th Circuit approved a class action settlement under Florida State Law saying that the fact that you had to spend 30 minutes on the phone to get your credit card replaced was enough to justify the settlement. The State Courts in West Virginia decided that even though the plaintiffs in the class action couldn't prove that they themselves were harmed and couldn't prove any financial damages, the fact that they might be at harm in the future based on their information being stolen was enough to justify a class action by the court.

There's another case where a California court just ruled to let the class action move forward because negligence was proven. They haven't yet proven their damages but it is moving forward because of negligence. That's why the standards that we've been discussing, whether they are state standards or FTC standards or NIST standards, having those best practices in place is going to be your defense, one of your defenses. If you are not at least meeting those standards, that case for negligence can be made.

Robert Owen: Let's open it up for questions. Judge Waxse?

Hon. David Waxse: How are you defining data breach and what equipment do you use to search for it?

Dale Zabriskie: Today, the term data breach is being defined as when there is an outside or inside influence that has caused material harm in removing or moving and obtaining information that is critical or has value to your organization. Data often gets exposed by people either doing stupid things or by systems opening up to the internet. I think the term is more defined around action that is malicious in its intent to release information whether it's a credit card that has specific intrinsic value or something that's more sociopolitical in nature. The key really is activity. Can an IT organization identify what is normal day-to-day on the network? If you can identify that and you have situational awareness, you can then identify what is abnormal.

"When you start to see certain ports open or certain transports taking place where data is moving at speeds which are not normal, hence, credit card information being taken off a system, that should alert an organization that there is an anomaly which needs to be addressed."

The key is data and being aware of the data. It's the only way it's going to be protected. That really was *Target's* issue. Not only did the bad guys get in through a 3rd party, *Target* didn't properly segregate the data on their systems. The conduit through the HVAC also ended up with access to the credit card information. *Target* could have segregated it better.

Peter Foster: Let me caveat that. Everyone talks about the big breaches. There is a case where a hospital had a breach of 21 paper records. There was an employee taking a file home on the subway and he left the file on the train. The conductor said, "I probably just threw it away." Each of the 21 patients had HIV or an STD. The $1,000,000 fine levied against the hospital came from Health and Human Services, OCR. The 21 suits were settled. That's a small breach but, to a hospital, it's a big loss. Everyone talks about electronic medical records, etc., and this was a paper file. So, it doesn't have to be an actual threat or an attack against your network.

"A data breach can be just simply, you lost the file."

Robert Owen: What is the computer system that's watching all this data flow? What is it they are looking at to determine whether a breach has occurred?

Dale Zabriskie: There's lots of different technology, some of which are built into networks. It tracks the flow of data across a network. You have got routers and switches and different things that make up a network that can detect movement activity, data transfer/data flow. They are also looking at copy data. Some of these technologies are built into things like the network itself. Others are forensics based and offer a visible log in system to view activity. They look at whether it's coming through a firewall or from a certain IP address. There are many different things that are put together to answer that question. At large organizations, the complexity is one of the greatest challenges.

David Shonka: One person I know has compared dealing with data security breaches and eDiscovery in this way: data security is eDiscovery on steroids. The point is that eDiscovery really deals with static information, files and things that are relevant to a claim or defense. Data security is looking at information in transit, in motion, and the ability to be able to detect motion that is abnormal and in the case of intrusions can be critical.

UNAUTHORIZED DISCLOSURE

CHRISTINA AYIOTIS: It's also data at rest. It's an unauthorized disclosure. If you don't have a right to access that information, then there's a breach. And, it doesn't matter what the format is. Some statutes, like HIPAA, went so far as to say that for protected health information, if you use the standard encryption approved by NIST and you lose something, even though you physically lost the data if no one can get to it, there hasn't been an actual breach. The corporate lawyers deal with that every single day.

DATA SECURITY INSURANCE

PETER FOSTER: There's insurance out there to protect you against this type of breach. We are seeing it more and more. It is *Target*, *Home Depot*, a number of the other major breaches had this type of insurance in place. It is only about 20% of corporations today that have the insurance. You can imagine the regulated companies today have that insurance. Manufacturing hasn't really purchased it but they are looking at it now because there is a focus on intellectual assets and protecting their value. From a data breach standpoint, it covers the regulatory fines, notification costs, credit monitoring, forensic costs, litigation costs, as well as settlements and judgments against you.

MANAGING DATA BASED ON ITS VALUE

DALE ZABRISKIE: With the exponential increase in threats that we have seen over the last decade or so, there has been a parallel exponential increase in the amount of data that exists in the world. It is just this immense amount of data and every company is dealing with it. As a CIO recently told me, "85% of my data is irrelevant" to which he added, "I just don't know which 85%." This is reality for organizations.

"YOU HAVE TO TREAT YOUR DATA LIKE IT'S CURRENCY."

Know what your $100 bills are. Know what the $50's, the $20's, the $10's, the $5's, the $1's and the coins are. When you do that, you can protect it effectively. You can back it up the right way. You can store it in the right place. You can put it in the cloud because maybe you don't care about it. You could even delete some of that data, which is one of the most therapeutic things any organization can do.

If you treat data like currency, you can get away from the blanket approach of back-up and security and secure things appropriately and adopt technologies, like the Cloud. Currency is the key. It is the currency of your world: it is data.

FINAL ADVICE

CHRISTINA AYIOTIS: Collaborate, collaborate, collaborate. Cybersecurity is a team sport. The legal department needs to work with security, needs to work with privacy. It needs to work with the C-Suite and with the different parts of the government.

MARK THIBODEAU: Mike Tyson once very eloquently said (some people actually attribute the quote originally to Joe Louis), "Everybody's got a plan until it gets punched in the mouth". I like the way President Eisenhower put it a little bit better, which is, "I have always found plans to be useless but planning indispensable." Have a plan for dealing with it. Make sure that plan involves the right inside and outside parties. Test that plan and test it frequently.

"IT SECURITY FOLKS OR ANYBODY INVOLVED IN SECURITY HAS TO GET IT RIGHT 100% OF THE TIME, EVERY DAY OF THE YEAR. A HACKER ONLY HAS TO GET IN ONCE. YOU WILL BE BREACHED EVENTUALLY."

ROBERT OWEN: All of us in the legal department now know what the threat landscape is and that it isn't just an IT problem. It's a problem that spans all of your organizations.

"GO BACK TO YOUR CLIENTS AND GIVE THEM THE MESSAGE."