Proceedings of the
2011 Legal Technology Leadership Summit
Amelia Island, FL
September, 2011

CORPORATE PERSPECTIVES ON

DATA BREACH & CYBERSECURITY

Adapted from a presentation on Data Breach and Cybersecurity at the **2011 Legal Technology Leadership Summit** by:




Christina Ayiotis, The George Washington University
Heather Enlow-Novitsky, Bank of America Card Services
Matthew Hagarty, AOL
Anthony Knaapen, Chevron Corp.

www.eDiscoveryInstitute.org

Overview

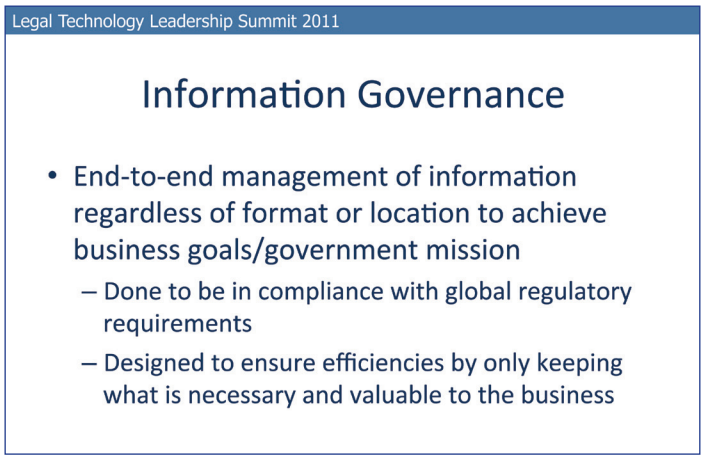
Data breaches and failures in cyber security can result in significant financial damages and reputational injury to corporations. The highly qualified panel members examine a number of processes and steps that can significantly reduce the risk of breaches or minimize their consequences. Topics included the importance of developing a written information security plan to minimize the risk of data breaches and to set out the steps to take in the event of data breaches; ensuring the security of data entrusted to outside counsel; vetting and contracting with vendors who handle or have access to confidential or private data; obtaining insurance coverage for data breaches; and data breach responsibilities for credit card merchants.

Note: This is an edited synopsis of a presentation made at the 2011 Legal Technology Leadership Summit. The views expressed herein are those of the presenters or of the EDI editors, and not those of the organizations with which the presenters may be employed.

Synopsis

The need to deal with data breach and cybersecurity holistically involving leadership from Legal, Records and Information Management, IT, Security and Compliance.

Ayiotis: I teach "Information Policy" within The George Washington University's Master's of Computer Science-Joint Certificate in Cybersecurity and Information Assurance program, and it has given me a perspective over the years as to how important data breach and cybersecurity has become and how it continues to evolve and become part of what organizations need to look at, holistically, with their Legal, Records and Information Management, IT, Security, and Compliance folks. "Information governance," is actually the term that pulls all these things together.



This content may be of most interest to:

- In-house counsel concerned about the security of information sent to outside counsel
- Law firm managers who want to meet the information security needs of their corporate clients
- Corporate managers who want to put a data breach plan in place
- Lawyers who advise businesses that accept debit or credit cards as payment for goods or services
- Risk managers concerned about the scope of insurance coverage available for data breaches

Individual Perspectives

Just to get started, each of the panelists will comment on their perspectives, and how their organizations look at things as well as the roles they have. Looking at the topic broadly throughout the organization helps mitigate the risk.

The Legal Department as Risk and Information Manager for the Data It Manages

Knaapen: For corporations, the law department or law function, should be the champion of information management, risk management, and compliance. We often look at data breach and cybersecurity as a business function – that as business partners, we are concerned about the data and the security of the information that we have when we use that in the business sense. We tend to focus on internal risk and interactions with our business clients, customers, vendors and competitors.

However, law departments are often not good about following through with their own retained counsel, and ensuring that retained counsel have adequate information risk management in their law firms. We don't necessarily follow through to see how they are handling the data that we give them. Without really thinking it through, lawyers tend to think well, what do I have to worry about with my retained counsel? They are my counsel, they are subject to all the confidentiality, attorney/client, work product privileges, so there isn't anything to worry about.

It's not how individual retained counsel use the information, but how that information is protected in their law firm, and what are they doing to ensure that the vendors that they pass our work on to are adequately protecting our data. So there's a whole huge continuum that goes beyond normal business use.

Legal has to really understand the risk because in today's world it's not a question of "if" you will be hacked, but "when" you will be hacked. And, it's important to understand how your company's infrastructure is set up so that you are not only able to reinforce policies with the business people, but in a litigation sense, that you're sure that your data is secure and that you're able to manage it well when you transfer data outside your company's control.

Hagarty: To follow up on Tony's point regarding the legal department as risk and information manager for data, be sure that Legal and IT coordinate—particularly on new and/or emerging technologies. As an example, organizations are flocking to the cloud as a way to cut cost, but technology teams must be made aware of certain risks associated with this this type of move and must also be patient while Legal builds proper contractual protections in the event of a data breach.

> "[I]n today's world it's not a question of 'if' you will be hacked, but 'when' you will be hacked."
> *– Tony Knaapen*

Credit Card Processing

Enlow-Novitsky: At Bank of America Merchant Services, we are a credit card processor, a joint venture between Bank of America and First Data, and so we look at data security from different angles. First of all, making sure that we're PCI DSS ("Payment Card Industry Data Security Standard") compliant, and secondly, assisting our merchants with their security. If our merchants are breached, we also assist them with the resulting fallout, forensic investigations, etc.

Corporate Culture – Innovation vs. Control; Avoiding "Compliance Complacency"

Knaapen: I think it depends a lot on your corporate culture as well as your company's core business. If you're really a technology company, obviously the motive is to be inventive, to be innovative, to be out there doing the latest things. If you're a more established company, certainly Chevron's been around for a 125-plus years, and something that has built gradually, you have the size and the infrastructure, the ability to build something, so our system is set up to be very controlled, to be very limited, to have a high level of security.

But companies easily fall into a compliance complacency and you think because you've done something once or you've looked at it once, it's adequate. Technology changes so quickly, that what used to be very secure on whatever bit encryption you had now can be hacked in five minutes so you constantly have to be up to date with what's going on in the marketplace and be able to integrate that and to budgetand plan for it in your IT infrastructure.

The Need for Continuous Monitoring, Collaboration and Risk Assessment

Ayiotis: Yeah, and certainly from a security professional's perspective, you want to have continuous monitoring. You want to have continuous risk assessment to figure out what the risks are. You have to have that collaboration, because I think that having that holistic approach and making sure from an industry perspective that you're sharing, collaborating and then within the organization, you've got all the slices. In fact, one of our competing sessions next door is about collaboration, and maybe the perspective is collaboration for e-discovery but I think that e-discovery is a slice of that bigger risk mitigation on the information side.

The Need for Cyber Insurance – The Sony—Zurich case

Ayiotis: We put in the presentation materials at the end the link to the article around cyber insurance, because a lot of folks think they have coverage for things that happen and don't realize that they actually need to get specialized coverage, and Zurich has taken the stance that the policies they sold to Sony don't actually cover the things that happen to Sony. It's worth looking at how that's playing out so that when you and your organization work and bring the folks together to say how are we mitigating this risk? How are we managing our information? How are we dealing with what the risks are today, and what kind of coverage do we have? What do the policies say, and if X scenario happens, is that going to be covered, there is some context. I'm guessing that at least in the financial services sector, everyone's pretty on top of how a breach response works and whether they have what they need to show that they've complied with PIN card industry standards which, by the way, I think are some of the most rigorous on the security side.

The Sony Data Breaches

Ayiotis: Sony had Play Stations and they had a breach, and then they also had multiple breaches afterwards, and to the extent that their insurers were all, I'm sure, thinking "Are we responsible for that, who's going to cover that?"

and all the investigations etc. So it really goes to the collaboration context within your organization. So the General Counsel, the CIO, the CFO, the Chief Risk Officer, and the Chief Security Officer if you have that, all having their respective teams looking at how are they are managing the information risk based on the kind of information and what is in place to ensure that that is meeting compliance requirements based on, data type and also the risk associated with it.

Technology Components and How Employees Use Them; Training and Auditing Employees and Outside Counsel

Knaapen: There are several components. One is you have, and take advantage of, the latest technologies. You offer various security mechanisms. You have smart badges, two-point authentication; you have encryption and you have certificates and various things, various ways to manage things technically within a company. But, under that, technology is no better than how your employees use it. Do they abide by password requirements; do they abide by how they're supposed to use their equipment? Have you educated and trained them, and do you have a system adequate to audit, to reeducate, to keep people up to date and hold them to the guidelines that are set out for the company?

Those principles hold true not only with the employees, but with retained counsel and service providers. If we have retained counsel set up and allow them access to a review tool that's on a special server, how do we audit, and we do audit, to make sure that they're not sharing passwords; that they're not taking information out of that system and doing improper things with it. And you have to put a process in place that assigns responsibility within the law firm, somebody to sign off that they are following your requirements and meeting expectations. And then you've got to report on it.

We've had people in some review situations where they've called in because they've had difficulty in accessing something from their home or doing something that they're not supposed to be doing; and to send a message reinforcing our policies, we've had our project manager pull the access for the whole firm, the whole group that was reviewing. We got a call in about 15 minutes from the partner saying what's going on, and we said, "Your people are not following our rules and regulations and you're putting our data at risk, and you can't do it that way." So, reinforce the message within your law firm that they have to do things properly, they've got to use the right passwords, they've got to access only from certain areas, and they have to be in secure locations.

So, technology isn't any better than how you use it and policies and processes you set up to take advantage of the technology. I think the weak spot for many corporation is employees accessing things in their e-mail, or going to a web site, or going to links that are phishingsites or scams or whatever, being careless; creating situations where unauthorized people might get access to company data. And depending on how well your company's infrastructure is designed, it makes you extremely vulnerable to hacking and attacking.

Thinking of the Entire Network and All the Connection Points

Enlow-Novitsky: I'd just add from the collaboration aspect that it's also important to think of your entire network, all your data altogether and all the connection points. Also evaluate how your network connects with the cloud, or your vendor's cloud. Companies may want to look at all pieces of their network and examine how all the pieces connect, as well as potential vulnerabilities.

Reiterating the Need for End-to-End Information Management

Ayiotis: Let me reiterate the need for end-to-end information management, in that context. So if you identify the data flow and you identify the creation or receipt point of certain data, you literally need to be mapping all the places where it will go, who will have access, what the systems are and what security controls are around that. That's a very, difficult process to do, but a necessary one. Because if you don't, then you have the scenario just laid out where someone figures out where that vulnerability, that weak point is, and they can get in and get access to the data without people even knowing, particularly because controls weren't put in place to monitor those pathways.

The Need to Have a Breach Response Plan In Place

Ayiotis: Having a breach response plan in place before the breach happens, before the crisis, is very important. And, to the extent that you have data with vendors, having contractual terms that deal with when something happens is important: how are they going to meet their obligations, and how are both of you going to figure out who is at fault (that's I think where some of the e-discovery forensics comes in, to say that you want to make sure that you do what you have to do vis-á-vis the customer vis-á-vis the regulators, but this is going to involve some costs and we've got to figure out ultimately who's going to bear those costs).

Dealing With a Credit Card Breach

Enlow-Novitsky: There's typically a lot of uncertainty when a breach occurs, so having a breach response plan prepared in advance that addresses how to escalate, and how to get the proper parties involved is useful.

If credit or debit cards are involved, merchants are generally required to contact their processor or the applicable card brand within 24-48 hours. You may also need to bring in a forensic auditor and/or law enforcement. There's proposed federal legislation by Rep. Mack that would require breached entities to notify affected individuals within 48 hours, and there are currently a variety of notification obligations under state law. So it's important to have that response plan to begin with, so that companies know what their obligations are and when they are required to notify certain parties.

As the investigation moves forward, companies may face potential investigations by state attorneys general, the Federal Trade Commission or other federal regulators, and potential litigation. In the case of the TJX breach a few years ago, TJX settled for $40.9 million with Visa and $24 million with MasterCard. The consumer class action litigation was settled for $6.5 million, and there was a $9.75 million settlement with the state attorneys general. So that is just an example of some of the costs in the case of a large data breach.

There is a lot of information out there, so if anyone has any questions?

State Attorneys General and Data Breach Litigation

Audience: Which state attorneys general were active the TJX settlement?

Enlow-Novitsky: It was the Massachusetts AG primarily, but 41 state attorneys general settled with TJX. Another example of liability as a result of a data breach is Heartland Payment Systems. They had a $60 million settlement with Visa, a $41.4 million settlement with MasterCard, a $5 million settlement with Discover, $3.6 million with American Express, and a $4 million settlement with cardholders. A lawsuit by their investors was dismissed, and the lawsuit by issuing banks against the acquiring banks was dismissed. The lawsuit directly by the issuing banks is still pending.

The Need to Have a WISP (Written Information Security Plan) – Especially if You Do Business in Massachusetts

Ayiotis: A WISP is a written information security plan. It's just an acronym. To the extent that states have lots of laws around breach notification, protection of social security numbers, too many that you all have to figure out when there's a breach of personal data, Massachusetts was the first place in the country to pass legislation to protect the personal data of its citizens in a way that requires any company that does business in Massachusetts and has information about people from Massachusetts. Is there anybody in the room that does no business in Massachusetts, that has no connection with the state?

It's rare to find such a company. So, in theory, every single company that did business in Massachusetts that had information about Massachusetts people needed to put a written information security plan in place; otherwise, they wouldn't be in compliance with the law.

Massachusetts Action Against Belmont Bank Over Missing Backup Tape – Need More Than a Written Plan

Ayiotis: Just a couple of days ago, the very first enforcement action was done against a bank, Belmont Bank, in Massachusetts that had an unencrypted backup tape that they left on the table overnight that the cleaning crew threw out in the garbage. They couldn't find it and they assumed that it was incinerated, but, and I don't know all the practice rules in Massachusetts, but they nonetheless issued something called an Assurance of Discontinuance, some kind of an agreement between Martha Coakley, the Attorney General and the bank. They also made the bank pay $7.5 thousand. The agreement also stated that if the data of the Massachusetts citizens should prove to be compromised in the future, if something happens, the AG warned "We're going to talk again" – fundamentally it's not enough just to have a written plan. You actually have to train your people and you have to have a program,you have to make sure you do what you need to do.

This really shows from a practical perspective if you're in-house, you really want to make sure that you're working with your HR people for your offices in Massachusetts to make sure that if they're asked in Massachusetts to demonstrate what's going on, there is a WISP. My recommendation is that your written information security program is a global one and takes into account all kinds of requirements, but in particular, you need to look to see that Massachusetts' requirements are met.

ISO and NIST Standards

Ayiotis: The law says you have to have all these things. You'd really better have all those things, even if you're just doing it in a narrow way because it is being enforced, and things are happening. And the requirements mirror information, ISO standards 27,001 and NIST 800-53r3, which are the U.S. government standards around security controls. They're not rocket science; they're not egregious. They're normal things, but it turns out that that it is going to be the trendsetter, just like California was the trendsetter for breach notifications. Then all the states followed suit. I think you're going see a lot of states moving in that direction and maybe even movement at a federal level. We've talked about the proposed legislation that really, I think, started out with the notion that we need to get breach notification to be consistent, but it's beyond just the normalization of breach notification requirements. It's also about being proactive on the front end.

The Need to Protect the Personal Data of Your Employees, Including in Contracts with Vendors

Knaapen: This issue involves everyone; we're not just talking about the good citizens of the Commonwealth of Massachusetts, but your own corporate citizens. Every company has lots of vendors engaged in business that includes the company employees' personal information. One, you really should be addressing internally proper information management and privacy policies. You should be defining the issues and concerns, expectations and responsibilities regarding privacy and personal data. You need to develop programs and processes to limit the number of people who have access to personal private information, and you need to educate your employees about the company's position on privacy. You should also be defining personal data, personal, private data and what processing means in your contracts with service providers and vendors who receive company data. Your contracts should also address any breach of information that relates to your own employees, including notification and remedies.

You want to protect your own employees from identity theft and anything else that might happen and you've got to have a plan ready for minimizing and for dealing with that internally, as well as dealing on a credit card issues or with external people's information.

Theft of Data by Employees

Hagarty: In addition to protecting your own employees from identity theft, it is also important to make sure data is not being removed by your employees—inadvertently or not. How can this be accomplished? Hiring practices and policies should be commensurate with the job responsibilities—do employees who are the stewards of an organization's confidential data have background checks performed? It also makes sense

to ensure proper security authentications are in place and that an employee has access permissions only for his or her role—the typical employee should not have administrator access to an organizations entire IT infrastructure. An organization should also have the ability to track usage and, where necessary, conduct internal audits.

In terms of inadvertent employee data breaches, a company should think about annual training seminars to go discuss the do's and don'ts of how to handle an organization's sensitive data.

Enlow-Novitsky: Certainly with employees, not only do you have to worry about protecting their privacy, but more to Matt's point, monitoring them and protecting their data especially with how easy it is to download data on to mobile phones and other devices.

Selecting and Auditing Vendors; Having Proper Contractual Language

Knaapen: On the vendor's side, we have a thorough and rigorous process to vet and select vendors. Our RFI/RFP s request a complete description of a potential vendor's security protocols, what security they have, what they use, whether their facilities are secured or not. The process includes an on-site visit to physically confirm that they have the security they described. We want to see that our documents are set aside from other clients; that it's not just a big open warehouse where different teams of reviewers have access to everything.

So, it's really important that you not only set certain expectations, but you follow-up and go and physically investigate. Confirm that what a vendor tells you is true, especially so that when you start hammering out the contractual terms and obligations, you know that they have the ability to comply with your requirements. You also need to monitor the work and make sure that there is recourse if a breach occurs. That is, if there's a data breach, they're giving you immediate notification of that breach. You need to know what steps they're going to take to remediate, and all of the process that goes along with that, as well as the costs involved.

Ayiotis: Matt, back to some of the relationships that you've managed over the years with different vendors, keeping track of who has what information and how they're managing it in terms of the copies they're making and the vendors they're using. Can you, speak a little bit to managing those relationships, especially when those vendors are keeping that litigation information that is so sensitive, some things that you've been looking at?

Vetting On-Site Vendors and Having Contractual Provisions

Hagarty: We keep a tight reign on data we send to vendors. Outbound data is catalogued and then encrypted if going through a courier. For smaller chunks of data, we will opt for data transfer via SFTP (Secure File Transfer Protocol). The preference is for the vendor to have the tools (hardware and software) on site so that they don't have to farm out to a subcontractor. Obviously, the goal is to limit the number of jump points the data has to travel.

Poking Holes in the Firewall

Hagarty: When monitoring network security, it makes sense to keep an eye on network traffic and restrict the use of Peer-to-Peer software. You don't want to provide a back door to your data, and this type of software has the potential to do exactly that.

Responsibility for Access Management Programs

Ayiotis: So, how many folks in the room work with or are responsible for their identity access management programs? Okay, just a few. So, now how many people know who the person is that manages that? Okay, a little bit more. It really should be everyone in the room if you're in-house legal or in-house information management or in-house security because you should be all working together. And, to the extent that when people, employees themselves come on board and are provisioned, someone needs to manage the information they're given access to so that as they change roles, they're only given what they need to execute their new roles and when they leave, that that's immediately cut off. Because in a lot of instances, organizations that are not on top of that leave themselves vulnerable to people who have left but still can get access, especially in this environment. Do you have a comment?

The Need to Have Contractual Right to Examine Source of Breach by Vendor's Computer

Audience: To follow on with what Matt was saying, another aspect of dealing with vendors we have had some unfortunate situations in this area where you find a problem; maybe it's a system trend, some malware, and it's coming in or emanating from a vendor, from an outsourcer who's on your network, you need a very clear definition of what investigation you can do.

We had a situation where an outsourcer had a problem. We detected the problem, we said, "You're on our network, give it up, give your machine to our forensic guys." They said, "No, you're not touching our machines; we've got our proprietary data there — we got other clients' proprietary data. You can't have it." We got into a huge tussle that took weeks to get resolved with lawyers; meanwhile, we didn't know what was going on on our network.

So, it's very important that when you have other people getting access into your organization, no matter who they are, that there's a very clear protocol of what your security people can do to correct the problem. Our security people looked at that situation, the vendor's security people found out. We finally got the machine and we found all kinds of things. So, you know that's one of those things where you do need to pay attention to that at minimum in your contracts: you're not putting that type of machine on your network.

Contracting and Auditing

Knaapen: Contractual terms are really important. You think it's not going to happen, or it's not a big deal, or we'll deal with it when it comes, and then you can't resolve it. So the contractual language is important and should include non-disclosure agreements, and the retention policies that relate to the data they receive. When the matter's resolved or the vendor's role is concluded, make sure they return your data, or provide a certification that they've destroyed it. You really have to think about all those things and cover them in your contract language, and then follow through with the audit. Because, again, the language doesn't do you any good if you don't go back and check it and confirm that they've met all the requisite obligations.

Negotiating and Drafting Contracts with Supply Chain

Ayiotis: And the people who are doing the negotiations within your supply chain need to be right next to the security, the records information management, and the legal folks, to make sure that everybody's on exactly the same page about exactly how this works. It's not just getting language in; you also need the certification and accreditation from a security perspective to ensure that the systems themselves have the requisite controls on them. The due diligence needs to be that collaborative effort of all the right people asking all the right questions and then saying to the vendor, "We're going to give you our data for this business function. This is what you do for us at this cost. You need to explain to us what other people besides your people may touch this information because there may be requirements in the EU regarding subprocessors so you'll need certain language put in place. You may need to get that locked down before you can finish your contract."

Those kind of things really require a knowledge of the end-to-end data flows and also who all the players are. Also, you need some level of control and strictness at the corporate level, on the corporation side, to make sure that even within their own corporation, people aren't going off on their own and doing stuff, and allowing people inappropriate or unauthorized access to the network, because that puts the network at risk.

The Need to Encrypt Company and Vendor Laptops

Knaapen: Within your corporation, your laptops, your computers may be encrypted; they should be encrypted, but do you require that of your vendors? If an employee loses a laptop, you're at least confident that your computers are encrypted, and it's going to be difficult for anybody to crack that and get to any data. That should also be a contractual obligation of the vendor if they're using laptops that have data from your company. We do have guidelines internally that any information at rest has to be encrypted. Is that valid? Do you have a way to audit that and make certain it's true? If you have people downloading to a thumb drive, are they educated about the fact that they should be encrypting those data? It feels comfortable to put that drive in your pocket and go home with it, but what if you lose that information and it contains personal information, HR, financial information? Your company needs to look at all those things, anticipate the problems and then reinforce your policies constantly through training and education, as well as through audits to make sure employees are following those requirements.

Management of IP and Trade Secrets

Ayiotis: One of the topics that we didn't put up on the slides, but I think that's increasingly important today, is the management of intellectual property and trade secrets, particularly the ability, when a trade secret is alleged, to show that you have in fact kept it secret, and you kept it secret because you control that information, its flow and where it's lived in very deliberate ways. This is particularly important because people take things with them when they're leaving. So, to the extent that that becomes a strategic issue in risk management for a lot of information-based organizations, they need to make sure they're managing that information because that information itself is an asset that has value and needs to be protected.

Use of Enterprise Search to Find Unsecured Privileged Content

Knaapen: We've actually got an interesting project that has a collateral benefit for our information management. We're trying to improve our ability to search across the entire enterprise to find data. During the implementation process we used the new search tool to find if there is information out there that should have been kept privileged or captive, or if it is someplace that's perceived to be not accessible but actually is. We can then identify these issues and then pull back the data and redesign processes to close the gaps and keep the stuff where it should be—accessible only to people that ought to see it.

The Need to Be Vigilant, Audit, and Have a Well-Defined Response Plan

Hagarty: Be vigilant. Make sure you've got your data locked down with various access controls . Make sure you've got some robust auditing abilities. Also, make sure that you have a really well-defined response plan that has all the key players identified and that should be included from the start should a data breach occur.

Many Breaches Caused by Common Data Security Flaws

Heather: Just to emphasize the point that a lot of breaches are still caused in whole or in part by common data security flaws: SQL injection, malware, or merchants using weak vendor passwords set to the default. These are examples of basic hacker methods, that have been known for a long time, but are still problematic, and there are relatively simple things companies can do to protect against these types of attacks and vulnerabilities. There is a lot companies can do to protect against breaches by keeping up with the basics.

The Need for Law Departments to be Supportive and Support by Example

Knaapen: Again, I think the law department needs to be supportive of its business partners to help them succeed in information management, privacy and security. Make sure you're using the right contractual language for terms and conditions of performance. Make sure you're supporting by example. Always audit the compliance practices you have and be available to help reinforce the goals and the objectives or your privacy and security policies broadly throughout the corporation as best you can.

The Need for Law Departments to Wisely Use Their Bully Pulpit to Mitigate Risk

Ayiotis: I'll reiterate something I've been saying for many years. If you are in-house legal and you have the bully pulpit, and you have the power within the organization to effect change, then support your records and information management people. You should support your security people. Advocate for them; listen to what they have to say. You should make it so that the message gets through; so that the support and the resources are put to manage those very simple issues. I mean, do basic educational things particularly with respect to "no tech hacking" and passwords and phishing. The biggest breaches that we've had recently in the news came from very simple things like e-mails where someone pretended to be someone else. And, those are basic security things that should have been Security 101, and everybody should know about it. Be an advocate and bring the players to the table, especially the ones who really have the knowledge but haven't had the power within the organization to be able to work together to say "You know what? Actually collectively, we do a great thing in meeting compliance and in being proactive around risk, at least as far as information is concerned."

Prospect for More Modern Secure Chips and PIN Credit/Debit Cards

Audience: The one particular thing I'd like to ask about, to Heather, is: "What is happening with respect to upgrading the old, out-of-date credit card payment system that's been around 40-plus years in order to bring it into the 21st Century where it's open and so that it's not so susceptible to every kind of breach? Really, I can see that our legal community and our technological community is doing a good job but it's extremely reactive and just not addressing the real underlying problem."

Knaapen: So, for those of you who may not have heard, he's asking what's being done to update the arcane credit card process in this country.

Enlow-Novitsky: If you take a step back and think about the payments ecosystem, there are way too many players, and they don't have the same resources, right? So, it's a big circle. There is the cardholder; there's you and me and we go into the Ritz-Carlton. We buy lunch and we swipe our credit card or our debit card, so the Ritz-Carlton is the merchant.

Then the payment network data gets transmitted to the processor or the merchant's bank. There are a lot of parties involved, and I'm going to call them all the acquiring bank who sends it off to Visa and MasterCard, who sends it back to your bank. So, if the card you swiped had Bank of America on it, they send it to Bank of America. Do they have the funds? Yea? Nay? Bank of America says yes, no, authorize the transaction. Then the data gets transmitted back. So, you have all these different parties to the system.

We all like to use credit cards, but think about your small mom-and-pop shop. If you want people to accept chip and PIN, you've got to start with the merchants. And the merchants are going to have to upgrade all of their equipment; a lot of them don't have the financial incentive to do that. Think about on the issuing side—not only do you have your big banks, your Bank of America, your Citi, your Chase, but you also have local credit unions. You have small regional banks. And, do they have the facilities to reissue all cards to all their cardholders that have this new technology? There are a lot of costs involved in order to get everyone on board to accept this new technology. Everyone realizes it's a risk and it needs to happen, but there's only so much you can force people to do.

Visa did recently announce that if you start accepting as a merchant chip and PIN payments, then you will not have to do PCI compliance. You will be waived for your PCI compliance and audit requirements for level one through three merchants. For a lot of companies, PCI compliance and PCI audits every year are a huge cost. So, it might be worth your while to start upgrading to this new equipment, to start accepting new types of cards so you can get out of that requirement. So you're starting to see the card associations try to think proactively on how to do that. You're seeing the chip and PIN issue become an issue in litigation. With Heartland and TJX, it was raised. If you don't have a claim, you didn't have good security. It's really a good way to incentivize everyone to get on board. They're trying, but it's going to be a slow process because of all the costs and players involved.

Audience: Just a simple follow-up: Why is it more secure?

Heather: So in the chip and PIN, it has the data encrypted in the little PIN in the card. Currently, the data in cards are in the magnetic stripe. In that magnetic stripe, when you swipe it, it has the full cardholder number, the expiration date and your CVV code. Most of us know it has that three-digit number on the back, or on American Express that four-digit code on the front. So, it's very easy if you capture all that data while it's in transit, because part of it, while it goes in transit, is unencrypted to the issuing banks. Then, you can take plastic cards. If I, Heather Enlow-Novitsky steal the data, I can take the data that I stole, manufacture new plastic cards that say Heather Enlow-Novitsky and that have all the different things that merchants are supposed to be checking, but I've stolen the magnetic stripe data earlier and put it into new cards so I make new cards. The chip-and-PIN system prevents all that.

Question: It's like two-factor authentication? Exactly.

Whether to Encrypt Everything

Audience: Two points that were made during your presentation: One was to encrypt everything and/or encrypt a lot of things; the other point was trade secrets have to be specially cared for, in order to be supportable as a trade secret. So, with that in mind, is it better specifically to encrypt only those things that are viewed as sensitive and to encourage employees not to encrypt the lunch menu or everything.

Ayiotis: A couple of comments to that. Not all information is created equal and it doesn't have equal value to the organization. So, there is a hierarchy of determining what's most valuable and what has requirements attached to it based on the data type. If it's personal data from the EU, it automatically has all these requirements attached to it if you want to be compliant, and you should be. If it's health information that is required under HIPAA to be managed in a particular way, baseline, you have all those requirements. Because the risk associated with that is so great, encrypting that, which if it's lost and it's encrypted, it's sort of simplistically a get-out-of-jail-free card, you're okay, it makes sense. Encrypting the lunch menu and all that other stuff which is of lower value in your organization or potentially publically available; you don't really need to apply the same level of controls.

The problem that organizations have is that they don't categorize, and they don't manage according to type of risk because it's hard to do that; it's all mixed together. So, by default, saying encrypting everything, it works — but it's expensive. Perhaps there is a middle ground going forward where you look at your systems; figure out what kind of data are in it; who's going to have access, and what the right controls are depending on what the requirements are, particularly the regulatory requirements and how important that is to your organization.

So very often, for example, in M&A situations in corporations, the people who do M&A work, they have stand-alone printers. They're not even connected to the network. They're doing whatever they're doing with outside counsel that doesn't even get that information, for all the right reasons. So, to the extent that you want to think about the information itself and manage the information in such a way that you're meeting the compliance and you shouldn't do overkill. I don't want the message to be that you should be encrypting everything. If you can afford to, fine — but it's expensive.

Encrypting With Other Parties – Consider an Encrypted Pipeline

Knaapen: If you're encrypting internally that's one thing, because that's an easier project than encrypting with other people, and you have to perhaps purchase the service to be able to encrypt. If you're doing a lot of communication, I'd recommend, if you can set it up, to set up pipelines with your retained counsel so that the line itself is encrypted, rather than just individual messages. I know that in e-discovery, you get into people'sfiles sometimes, and you've got a thousand individually encrypted messages. Each of those has to be decrypted separately and it's a pain. So, there are different ways to approach it and I guess, depending on what you're dealing with, the volume and the different types of information, there are different ways to deal with encryption and you should look at those.

Don't Keep What You Don't Have To!

Ayiotis: And the other thing I can't resist saying- I'm sorry, I'm a certified records manager- Don't keep what you don't need to keep. This is part of the problem. This is why a multi-billion e-discovery industry arose, because there was so much information, and most of the judges in this place will tell you that of the hundred thousand documents that you collected, ten decided the case; there's a awful lot of information that's un-necessary and it's duplicated, and it has to do with not having up front at the high level, the information governance in place and the ability to manage. I think with the increased costs with data breaches and cybersecurity, organizations are going to be better about managing their information. They're going to be better about saying, "Do I really need to pay all that money to encrypt all that; do I need all that stuff?"

If, within the organization, you push some of the responsibility and costs back on groups, who say storage is cheap, remember, they forgot the hourly rate of the review; when calculating the cost of storage, they were just talking about the hardware. They said if you want to keep all this information, this is what it's going to cost you, because I've got to put all our security information on top. Well, do we really need to keep all of that? And it makes them more disciplined. Now for those of you who make their living off the information mess, I'm sorry.

Further Information

- The Sony data breach insurance coverage question involving Zurich:
  reut.rs/EDI_Sony_Ins
- ISO standards 27,001:
  bit.ly/EDI_ISO
- NIST 800-53r3:
  1.usa.gov/EDI_NIST
- Gordon Hilliker, "Cyber Risks and Liability Insurance," *The Lawyers Weekly*, August 19, 2011:
  bit.ly/EDI_Cyber_Risk_Insurance
- Nick Ackerman, "How Do You Sue an Unknown Hacker Who Steals Data through the Company Web Site," Computer Fraud/Data Protection,
  Dorsey & Whitney LLP, Feb. 7, 2011:
  bit.ly/EDI_Suing_Unknown_Hackers

This publication is part of a series of Proceedings published by the Electronic Discovery Institute.

Electronic Discovery
INSTITUTE

About the Electronic Discovery Institute

The Electronic Discovery Institute ("EDI") is a 501(c)(3) non-profit research and educational organization dedicated to identifying effective legal technologies and processes and teaching lawyers and judges about their use. As part of that mission, EDI conducts studies and surveys to provide cost and quality metrics on different technologies and processes, hosts forums such as the Leadership Summits which permit lively interaction with thought leaders in legal technology, and provides educational programs for practitioners and judges.

All EDI publications are free and available on the EDI website at www.eDiscoveryInstitute.org