THOUGHT LEADER FORUM

Cyber Security

*As data breaches continue to occur with alarming frequency, cyber security issues are on the minds of area business owners and leaders. Puget Sound Business Journal Publisher **Emory Thomas** recently held a Thought Leader Forum discussion about cyber security and what companies can do to protect themselves from this threat with two area attorneys: **Kurt Hermanns** of Gordon Thomas Honeywell and **Darin Sands** of Lane Powell. A summary of their conversation follows.*

Are you finding your own clients are deeply engaged with cyber security issues or do they need to be pulled into awareness?

HERMANNS: Larger business clients have made this a priority. For medium and smaller sized companies who are at the beginning of the learning curve it's a daunting challenge. A lawyer's perspective can give them the framework to have defensible policies in place if they have a breach and regulators come knocking.

Do you think many CEOs are unaware of the steps they need to be taking?

SANDS: There are contractual issues, particularly indemnification issues, that people aren't looking at as hard as they need to. There also are international obligations – the European GDPR (General Data Protection Regulations) is going into effect next May which have substantial financial consequences for companies that have European customer data on their servers. You don't have to be operating in Europe for those regulations to attach.

HERMANNS: The last time I checked there were 48 states that had separate statutory schemes related to cyber security. There are 16 separate federal statues and huge differences in philosophy over cyber security issues between countries. Russia takes a position that any data that passes through their country using a server within their territorial boundaries belongs to Russia. With this complexity, it is a difficult task for CEOs to monitor changes and stay informed of the steps they need to be taking to protect their company and their customers.

That is unbelievable.

HERMANNS: It's a little staggering.

SANDS: China just passed a data security law that is horribly ambiguous and drafted in a way that raises serious concerns for any company with customer or company data in China. It's increasingly difficult for a lot of clients located in the US to have cross border data transfers, which happen all the time. Just because you are located here and your operations are here doesn't mean you can look the other way when it comes to international data security and privacy regulations.

I'm a CEO of a small to mid-size company who has decided I need to educate myself, jump in, and start reducing the risk on this front. What are my first steps?

HERMANNS: My advice would be to hire us first. That's not entirely selfish. The laws surrounding cyber security are elaborate and changing rapidly. I think from an analytic framework the very first issue a company new to cyber security needs to address is its current obligations under existing law.

What is the most common cyber security threat for companies?

SANDS: Any size business is potentially subject to attack. A large range of businesses hold intellectual property, credit card or health care data that is valuable on the black market and subject to attack. A company should not think it can fly under the radar. Even if you don't get sued or catch the attention of regulators, the biggest threat is loss of business operations and damage to customer trust because most companies require breach notifications. Also, be aware of increasingly vigilant state regulators who are seeking to crack down on companies that aren't taking this seriously.

> ***"The biggest threat is loss of business operations and damage to customer trust because most companies require breach notifications."***
>
> **DARIN SANDS** | Lane Powell

What is the most common source of the threat? Who are the typical perpetrators? Are they offshore crime rings? Two 15-year olds in a basement?

SANDS: Unfortunately, the marketplace for hackers is global and there are elaborate crime networks, mind-boggling in their geographic scope. There are organized crime networks in the US and in Russia. State actors are a huge factor. The Chinese, North Korean, and Russian governments have all been behind high profile attacks on American companies.

What is a "NIST compliant plan" and how does it benefit a company that has a cyber security breach?

HERMANNS: A NIST compliant plan is a product of an executive order issued by President Obama in 2013. It directs the National Institute of Standards and Technology to work with private industry and government to create a set of best practices and agreed upon standards. It's a very useful effort.

SANDS: It's an attempt to provide a road map to give companies a flexible framework to operate in with the knowledge that if they do that they are clearing a minimum threshold. My frustration is that we don't have more safe harbors built into law to let companies know that if they do that that they aren't going to face legal consequences if there is still a breach.

Do attorneys tend to work closely with consulting firms to advise companies on cyber security? How closely do you work with those firms?

HERMANNS: Once the applicable statutory standard of care is identified, the law firm brings in the tech company to look at the business systems. This structure provides some protection in terms of attorney/client privilege to the client. Sometimes a company views cyber security as strictly a technical problem and brings in only a tech company. But if there is a breach later, that information can become discoverable. We want to ensure the most protection for the client which is why the law firm should secure the tech firm in furtherance of giving legal advice.

SANDS: The question of when attorney/client privilege attaches to pre-breach prep or post-breach response is a tricky one. I do agree that hiring vendors under the attorney/client privilege, especially in a breach response effort, is critical. Pre-breach, there are times when it's appropriate and there are also situations when you want to prove you've been doing these things and you don't want to shield that with privilege. I encourage lawyers in cyber security to be very collaborative and to recognize the strengths of other professionals and find a thoughtful place at the table as lawyers so they can contribute throughout the process

HERMANNS: What we need to avoid is a client learning about cyber security liability after a breach has occurred. With some risk management planning, we can show that you're aware of the problem, you've followed legal advice, you've had a tech review, and you've had a NIST review. These steps can help minimize or perhaps avoid liability.

What role does attorney-client privilege play in a data breach investigation, particularly if there are other outside parties involved in these conversations?

SANDS: This is critical. This is why you have a breach response plan in place and a lawyer on the team. Ideally, in a breach situation, legal counsel would be called first and they would engage a tech forensic vendor, investigators and potentially a PR firm to deal with post-breach response. This enables a company to have those critical discussions immediately after a breach in a way that's protected by privilege and allows people to act freely and quickly and not have soundbites or information taken out of context later if they're sued or pursued by regulators. I can't tell you how many situations we see where communications in that first 24-72 hours are used as evidence of liability.

What is the effect of news coverage on this area? How have these conversations impacted what you do?

HERMANNS: It has little impact on small to medium-sized businesses. They often think they are too small – they are not Sony, Home Depot, Target – and they think they're off the radar, which is false. They also think they cannot afford a cyber security review and that for them to have any kind of credible cyber security plan they've got to hire the biggest law firm and make expensive tech investments. We need to get to a point where companies consider cyber security the same way they do any other risk management issue and integrate it into the overall management of their firm.

What are your firms doing to ensure that you have the experience on your staff and the increased capacity you may need to address this for your clients?

SANDS: Data is increasingly the most important asset of most businesses and is central to operations. It is also one of the biggest areas of legal risk as it touches on everything, not just cyber security. Kurt and I are data lawyers and in the next ten years every lawyer will have to have some fluency in these issues because it will not be siloed in the legal profession in the future.

Any closing words?

HERMANNS: It strikes me as unusual and frankly extraordinarily unfair that the burden of protecting our electronic information is placed on the shoulders of the user. In other industries – like automotive – we don't put the burden on the car owner or driver to create a safe automobile. Using an attorney and a technology consulting firm is a beneficial way to alleviate a bit of that burden.

SANDS: One thing small and medium size businesses can do is move their IT operations to the cloud. There are legal issues around that and certainly you have to do your diligence but one advantage of using a cloud service is that they are better equipped to deal in a threat landscape.

THOUGHT LEADERS

DARIN M. SANDS

Shareholder | Lane Powell
sandsd@lanepowell.com
503.778.2117

LANE POWELL

Darin is Co-chair of Lane Powell's Privacy and Data Security Practice Group and currently represents numerous companies in ongoing data breach litigation and data breach response preparation efforts. Darin also frequently counsels clients on privacy-related legal challenges. He is a member of the International Association of Privacy Professionals and is frequently asked to speak at privacy-focused conferences throughout the country. Darin received his J.D. from Harvard Law School, where he served as Editor for the Harvard Journal of Law & Technology.

KURT HERMANNS

Attorney at Law
Gordon Thomas Honeywell LLP
khermanns@gth-law.com
253-620-6518

GORDON THOMAS HONEYWELL

Kurt is Of Counsel in the Tacoma office of Gordon Thomas Honeywell. He joined GTH after a lengthy career with the United States Attorneys' Office for the Western District of Washington focusing upon complex crimes ranging from securities frauds, investment schemes, tax cases, real estate swindles and cyber crimes. His practice at GTH focuses upon criminal related risk management issues for South Sound businesses. His practice also includes assisting clients in addressing cyber security risks, the applicable legal duties and working in conjunction with a tech partner to create NIST compliant plans.