Running With Scissors

Trends Suggest that Cyber Loss are On Track to Becoming One of the Most Significant Exposures Facing Companies In Years

Michael S. Hale, J.D., CPCU, AAI
Melissa L. Hirn, J.D.
Risk Management & Insurance Coverage Counsel

Clairmont Advisors, LLC
Insurance & Risk Management

About
THE AUTHORS

phone: 248-321-8941
fax: 248-692-4012
email: info@clairmont-advisors.com

INSURANCE & RISK MANAGEMENT COUNSEL

Michael S. Hale
J.D., CPCU, AAI

Michael S. Hale has been a practicing attorney for 20 years. During that time he has specialized in insurance coverage and risk management related matters. After years of experience as CEO of a large independent insurance agency, he formed Clairmont Advisors, LLC in 2013 as an insurance and risk management consulting firm where he manages commercial insurance programs. He has served as an expert witness in over 150 cases. He is a 1989 graduate of Hillsdale College and a 1994 graduate, *cum laude*, of Michigan State University School of Law.

Melissa L. Hirn
J.D.

Melissa L. Hirn has been a practicing attorney for almost 20 years. She is a 1991 graduate, *magna cum laude* of Western Michigan University and a 1995 graduate of Dayton University Law School. Ms. Hirn has been a judicial attorney for a Wayne County Circuit Court Judge and is a regular columnist in the monthly publication, *Insurance & Risk*. She is risk management counsel to 360 Risk Management, Inc. located in Northville, Michigan. As a licensed property and casualty insurance agent she assists businesses in managing their risks and insurance programs. She is currently in the process of completing her Accredited Advisor in Insurance (AAI) designation.

Clairmont Advisors, LLC
Insurance & Risk Management

Introduction to
CYBER EXPOSURES & COVERAGES

This white paper is about the Wild Wild West of the 21st Century where computers and the Internet are the means by which crime occurs on a regular basis. The constant morphing of the protocols of cyber criminals using the latest technology to steal money, data and to extort even baffles some information technology specialists. It seems as though anything goes.

This has become a national concern. In 2014, *The New York Times* devoted more than 700 articles to data breaches compared to fewer than 125 in 2013.[i] In fact, October is the designated U.S. Department of Homeland Securities National Cyber Security Awareness Month.[ii]

According to some experts, computer fraud through the unauthorized access of data or funds is going to advance into one of the largest exposures facing businesses and could be the tool for the next national terrorist attack or other disaster.[iii] These risks are concerning. The potential casualties are company bank accounts, profits, computer systems, data and business reputation.

The purpose of this paper is to present some statistics and real-life exposures to illustrate what can happen to small, medium and large businesses and to provide information on insurance coverages available to address these exposures. To put it in its proper perspective, check out the following website to see real time computer hackers at work in attempting to penetrate computer networks throughout the United States: **map.norsecorp.com**.

One thing we have learned in the study of these exposures and the insurers offering such policies is that there is a wide-array of differences between the types of coverages being offered.

We have titled this paper *Running with Scissors* because this is exactly what we find many companies, especially the smaller ones, doing when faced with cyber risks. Many executives believe that their companies are immune to such exposures if they do not handle credit cards or medical information and that the risks are limited to the multi-national corporations. We say this because this is what we frequently hear from our clients and other companies we work with.

An increasing number of Directors & Officers liability insurers are excluding anything related to cyber liability. To make matters worse, such policies often exclude wrongful acts in securing or failing to secure insurance coverage.

Those companies not only avoid buying cyber coverage, they often overlook updating systems such as firewalls and implementing other safeguards to avoid computer-related losses. Our research suggests that this is just as if the executive is running with scissors.

We find that many small to medium sized companies have not sought out the purchase of cyber coverage in any form although they are some of the most frequently targeted companies. However, even if they do, it is not that simple. There are more and more insurers offering these coverages either via separate cyber policies or, less effectively, as an add-on or throw-in to business owner's basic general liability policies.

On average, the FBI receives over 20,000 complaints of cyber crime every month.

One thing we have learned in the study of these exposures and the insurers offering such coverages is that there is a wide-array of differences between the types of coverages being offered. This is perhaps more so than certain other types of property and casualty insurance policies. This analysis was a revelation and certainly this complexity is going to continue to develop as the exposures warranting the coverage change.

We have found that at the time of a cyber claim, many insurers look carefully at the applications submitted by the insured to ascertain whether the procedures represented were actually implemented and if they were not, some carriers are denying coverage and seeking to rescind policies. Cyber insurance applications can be daunting and the chance for error in representations on these forms seems to be easier than one might think.

Cyber exposures are far from static. Aside from having a qualified IT Department and an outside consulting firm, organizations would be well advised to utilize insurers and agents who know the policy differences and can properly advise them.

What's in the **WILD?**

On average, the FBI receives over 20,000 complaints of cyber crime every month. In 2014 the total losses reported totaled $800,492,073. Although Michigan did not make the list, two states in the Midwest were among the top ten states affected by cyber crimes in 2014. Business e-mail compromise scams resulted in reported losses of $226 million dollars in 2014.[iv]

Check out the following website to see real-time computer hackers at work in attempting to penetrate computer systems throughout the United States [map.norsecorp.com].

In its 2105 Data Breach Investigations Report, Verizon, along with 70 other organizations from around the world, determined that a whopping 60% of cyber incidents were caused by system administrator oversights.[v] Making matters worse, many cyber incidents take days or weeks to discover.

In 2014, the evolution of attacks against Point of Sale (POS) continued, with large organizations suffering breaches alongside the small retailers and restaurants.[vi] The extent of the complexity of computer systems and firewalls appear to be no match for sophisticated cyber criminals.

60% **In its annual study, Verizon determined that 60% of cyber incidents were caused by system administrator oversights.**

One expert recounts an example of a hacker placing a thumb drive with a one hundred dollar bill rubber banded around it on the sidewalk outside the headquarters of a major company at 8:00 am on a business day. The hacker was counting on someone to pick it up and insert the thumb drive into a corporate computer along with the unintended malware which it contained.

In another recent claim we were consulted on, a hacker intercepted an email and changed the wire transfer instructions on a client Adobe document, making off with over $200,000.

Social engineering claims are becoming more and more common as cyber incidents.[vii] These claims refer to psychological manipulation of people into performing actions or divulging confidential information. It is one of the steps in a more complex fraud scheme.[viii] Some insurers are now offering coverage to address this exposure.

Clairmont Advisors, LLC
Insurance & Risk Management

One expert recounts an example of a hacker placing a thumb drive with a one hundred dollar bill rubber banded around it on the sidewalk outside the headquarters of a major company at 8:00 a.m. on a business day.

Most have heard of the cyber breach at Target Corporation where the information of hundreds of thousands of customers was obtained by hackers. Many do not know that this was actually a breach into the systems of one of Target's vendors through which the computer hackers were able to get around Target's firewall.

Service providers are also at risk. According to *Legal Tech News*, law firms have significant exposures for cyber claims given the sensitive and confidential information that they maintain. A single breach could destroy the reputation of a law firm.[ix]

CYBER-EXTORTION: Sometimes it's not just about the money

The recent scandal involving the Canadian-based website Ashley Madison has garnered international attention for the breach of 39 million membership files and is now the subject of multi-million dollar lawsuits in Canada and the United States.[x] There, the hackers initially were not using cyber-extortion to steal money. Instead, their threats were a means to shut down the site as punishment for collecting a fee without actually deleting user's data.

CYBER EXTORTION CLAIMS ARE MORE COMMON THAN MANY BUSINESSES THINK. THEY GENERALLY INVOLVE:

- **Threatening a hacking attack or virus into the company's computer systems;**
- **Threatening to disseminate, divulge or utilize information contained or once contained in the company's computer systems; or,**
- **Threatening to damage, destroy or alter the company's computer systems.**

Interestingly, some of the cyber policies we reviewed may not have covered the Ashley Madison incident under the cyber extortion coverage part because funds or property were not demanded. It is likely that this company incurred considerable fees and expenses of consultants in attempting to find the extorters and otherwise managing the extortion. However, the breach itself would likely have been covered.

Clairmont Advisors, LLC
Insurance & Risk Management

We see many small to medium-sized business executives roll their eyes when presented with the exposures associated with cyber attacks. Yet a gigantic 31% of all cyber attacks in 2014 involved companies with 250 or fewer employees.

We see many small to medium sized business executives roll their eyes when presented with the exposures associated with cyber attacks. They may not know what they could be facing. According to a recent article in *Plante Moran's Engage Magazine,*[xi] Cyber Security Partner Raj Patel, states that companies with 250 or fewer employees accounted for a gigantic 31% of all cyber attacks in 2014. This means cyber exposures apply to you.

>> IT'S NOT JUST THE BIG GUYS THAT ARE BEING TARGETED

REASONS TO CONSIDER CYBER COVERAGE:

- Protects against claims against your organization by other individuals or organizations because of a cyber event (third party losses)
- Pays for your losses (first party losses) because of a cyber event
- Assists you if there is a cyber event

In some cases, buying the right insurance coverage may seem as complicated as the schemes it is designed to address.

Going bare on cyber exposures is risky but even if you are going to buy coverage, you better have an insurance expert.

COVERAGE HIGHLIGHTS AVAILABLE UNDER CYBER POLICIES:

Third party cyber liability coverage for:

- **Disclosure injury** including lawsuits alleging unauthorized access to or dissemination of the plaintiff's private information. (Can be extended to outsourced data processing and data storage services.)
- **Content injury** including suits arising from intellectual property infringement, trademark infringement and copyright infringement.
- **Reputational injury** including suits alleging disparagement of products or services, libel, slander, defamation, and invasion of privacy.
- **Conduit injury** including suits arising from system security failures that result in harm to third-party systems.
- **Impaired-access injury** including suits arising from system security failure resulting in your customer's systems being unavailable to its customers.

First-party cyber crime expense for:

- **Privacy notification expenses** including the cost of credit-monitoring services for affected customers, even if state law doesn't require it.[1]
- **Crisis management and reward expenses** including the cost of public relations consultants.
- **E-business interruption** including extra expenses incurred by the organization.
- **E-theft and e-communication loss** extended to networks outside of your company's system.
- **E-threat losses** including the cost of a professional negotiator and ransom payment.
- **E-vandalism expenses** even when the vandalism is caused by an employee.

[1]The notification costs to notify 39 million potentially affected parties at an average of .30 cents per notice would be a staggering $11,700,000.

Failing to follow policies and procedures you referenced in the application could come back to haunt you at the time of a claim. Insurers are denying coverage on this basis.

Cyber insurance policies are not all created equally. As more and more insurers enter this market, understanding the available options among policy forms becomes a challenge.

Many executives do not know that acts or omissions they make relative to cyber risks are not likely covered by D & O policies. First, many D & O policies exclude any claims arising out of inadequate insurance. Secondly, most D & O carriers are adding total cyber exclusions to such policies.

The process of securing coverage, or at least a quote, starts with completing a required application for insurance. These applications for this kind of insurance pose big concerns. Failing to follow policies and procedures you referenced on the application could come back to haunt you at the time of a claim. In real-life, insurers are denying coverage on this basis. See "Insurance Applications Pose Risks," *EnterpriseTech*.[xiii]

Some of the basic required protocols built into many of these policies are:

- Procedures for changing the firewall default password.
- Installing patches or updates within 60 days of availability.
- Ongoing system and network monitoring.
- Procedures for off-site data handling i.e. laptops and tablets, remote access.[xiv]
- PCI update compliance for credit card merchants.

If the procedures stated in the application are not followed, cyber insurers may look to deny coverage.

Clairmont Advisors, LLC
Insurance & Risk Management

Top Concerns about
CYBER & RELATED COVERAGES

We recently did a comparison of certain key coverages among a number insurers writing cyber policies and the result was eye-opening to say the least. We find that most businesses are simply not properly covered for computer fraud or cyber exposures. **Even if they do secure coverage, we run across many issues including:**

- Many insurance agents do not understand the intricacies of cyber coverages and are ill-equipped to advise companies on these exposures. The agents we typically interact with tend to believe that one size fits all for cyber coverages. In part, this is due to the relatively recent heightened awareness of these exposures and the fact that many insurers are broadening the scope of the coverage offering.
- Even if a cyber policy is secured, many organizations remain naked when it comes to the proper crime coverages such as social engineering, computer and electronic fraud and false pretense coverage.
- The plethora of coverage options is daunting to say the least. See our checklist of some of the things we look for at Appendix A to this paper.
- There are more and more insurers offering a form of cyber coverage all the time. Some do not compare to the main players in terms of the coverages provided. This includes "throw-in" coverage on businessowner ("BOP") policies. In these cases, typically only liability coverage is included without any of the first party critical coverages like notification cost expenses.
- Some companies, particularly in the technology arena, maintain cyber coverage as an add-on to their professional liability coverage. This may not be the best solution as it may require a link to performing professional services for clients whereas cyber exposures may not involve this.
- Some cyber policies do not extend coverage if you are working on computers of others at their locations.
- Many insurers who are offering cyber coverage may have general liability claims adjusters handling claims. This is often times less than desired. These claims are complicated to say the least and you would want a seasoned adjuster dedicated to cyber claims to help get your organization through the nightmare.

Is the Board of Directors asking for a cyber exposure report it can understand? There is now software available which will pinpoint sensitive information on employee computers. This type of information is invaluable in negotiating favorable cyber policy terms and conditions.

Top Concerns about
CYBER & RELATED COVERAGES

(concerns-continued)

- Many insurers will offer what can be important risk management services without further charge. This can be critical at the time of a claim when loss mitigation is vital. However, insurers differ widely in what they will offer.
- Some companies use the purchase of cyber coverage as their only risk management tool. Having a dedicated IT person or department and a qualified outside IT consultant are critical components of the overall plan. Experts advise that for purposes of objectivity, an audit should be done by a firm different than the IT firm normally used. These specialists should assist in developing a written cyber plan, including disaster recovery and denial of service contingencies.
- Not understanding what specific cyber exposures the company may have is a big issue. There is now software[2] available which will pinpoint sensitive information on employee computers. This type of information is invaluable in negotiating favorable cyber policy terms and conditions.
- Applications for cyber coverage are often completed by the person responsible for buying the insurance at the company without the input of the IT department or outside experts. As noted above, at the time of a claim many insurers will look carefully at whether the stated controls have actually been put in place and maintained. The information on the application must be completely accurate.

Check with your insurance professional on the extent of your coverage or contact us for a review of your policies.

Clairmont Advisors, LLC
Insurance & Risk Management

Appendix A
I CAN BUY INSURANCE FOR THAT?
CHECKLIST OF CYBER COVERAGES TO CONSIDER

- ☐ Information / Security and Privacy Breach Covered?
- ☐ Regulatory Defense and Penalties Covered? Unlimited or Dollar Limit?
- ☐ Website Media Liability Covered for Publishing Protected Material?
- ☐ PCI Fines Covered?
- ☐ Cyber Extortion Covered? Limit?
- ☐ Data Protection Loss Covered?
- ☐ "Open Peril" Policies for Security / Privacy Wrongful Acts Apply?
- ☐ Rogue Employee Carve-Back Covered?
- ☐ Definition of Damages Included Punitive / Exemplary Damages?
- ☐ Costs for Both Voluntary & Involuntary Notification Covered?
- ☐ Per Person vs. Monetary Sublimit?
- ☐ Breach Costs Outside Aggregate Limit?
- ☐ Notification – Third Party Cut-Through?
- ☐ Broad Definition of Personally Identifiable Information / Confidential Information?
- ☐ Is a Denial of Service Attack Directed Against a Third Party Computer System Covered?
- ☐ Business Interruption / Loss of Income Due to a Cyber Event Covered?
- ☐ Public Relations Consultancy Costs Covered?
- ☐ Bodily Injury or Property Claims Arising Out of Breach Covered?
- ☐ Distribution of Unsolicited Email or Facsimiles, Wire Tapping or Telemarketing Covered?
- ☐ Social Engineering Coverage for Phishing Claims Covered?
- ☐ Employee Dishonesty Coverage for Employee Stealing Covered?
- ☐ Coverage for Computer Fraud / ETF for Unauthorized Transfers to Outsiders?
- ☐ What Are the Risk Management Services Offered as Part of the Coverage Plan?
- ☐ What is the Cyber Claims Expertise of the Insurer?

Clairmont Advisors, LLC
Insurance & Risk Management

RESOURCES:

(i) *2015 Verizon Data Breach Investigations Report*

(ii) www.dhs.gov/national-cyber-security-awareness-month

(iii) Alex Burkulas, Cygnus Systems, Inc.

(iv) www.ic3.gov/media/annualreport/2014_IC3Report.pdf

(v) Id

(vi) *2015 Verizon Data Breach Investigations Report*

(vii) ***Claims Connection*** Article 8/12/15,
www.propertycasualty360.com/2015/08/07/social-engineering-scams-how-hackers-are-stealing

(viii) en.wikipedia.org/wiki/Social_engineering_(security)

(ix) m.legaltechnews.com/article/1751945512

(x) ***The Financial Express***, August 24, 2015.
www.financialexpress.com/article/industry/tech/ashley-madison-faces-578-mn-canadian-class-action-lawsuit-over-adultery-website-hack/123894/

(xi) www.plantemoran-digital.com/plante-moran-engage/engage_issue_2_2015#pg16

(xii) www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf;
www.pcicomplianceguide.org/five-pci-dss-3-0-best-practices-about-to-become-requirements

(xiii) www.enterprisetech.com/2015/07/15/the-truth-about-cybersecurity-insurance/?kui=xEMgQwJfzQf-Cjni-YMUkA

(xiv) Mike Pittenger, vice president of product strategy for Black Duck Software, Burlington, Mass.