# Your Coverage Advisor

Insurance Coverage Newsletter
Spring 2017 (Vol. XV)

## A Matter of When Not If – An Equipment Failure Policy Could Help Tame the Unpredictable

*By Andrew Rowles*
*arowles@seibertkeck.com*
*SeibertKeck Insurance*

Imagine a late summer day, it is 90 degrees and 100% humidity. From inside your office you hear a loud bang as a pole top transformer explodes just down the street from your building. Not much of a concern, until seconds later an artificially generated power surge comes through the overhead utility service line, taking out your second leg power feed for production equipment, shorts out the $11,000 rooftop air-conditioning unit, and you lose power. Almost instantly, smoke starts to engulf your production facility and you realize you are not going to have a relaxing afternoon. Your business depends on functioning equipment to operate and maintain revenue, so a breakdown could be devastating. You begin to panic. As the smoke triggers the alarms, you realize that being a just-in-time manufacturer means every minute of downtime results in missing a customer's deadline, a new order, and loss of revenue.

The threat of breakdown is increasingly prevalent in your organization because technologically advanced equipment tends to be sensitive, fragile, and can easily sustain damage from occurrences outside of your control. While this is a hypothetical scenario, today's organizations rely heavily on the consistency of the utilities servicing their facility. In response, the insurance industry provides insurance policies to address equipment breakdown and utility service interruption that results in damage to critical production components. Equipment Breakdown insurance policies encompass more than utility service interruption. They can include coverage for direct property damage, extra expenses needed to restore operations, loss of revenue, replacement of perishable goods, hazardous substances removal, data restoration, to mention a few. Here are a few examples of critical components:

**(Continued on page 2)**

## IN THIS ISSUE



BROUSE McDowell®
A Legal Professional Association

## A Matter of When Not If... **(Continued from page 1)**

- **Technology equipment provides a host of invaluable features that can include circuitry on high-tech equipment. A breakdown in telecommunication could mean lost time and revenue.**
- **Electrical systems make up 10 to 15 percent of a building's worth, so a short circuit in a transformer or panel could quickly destroy a large part of the system.**
- **Air conditioning and refrigeration systems are critical components for many industries, so damage to these units could temporarily suspend operations.**
- **Hot water boilers are subject to cracking, collapsing, bulging, and explosion. If your building loses heat in the winter because of a faulty boiler, what is your contingency plan?**

Historically, equipment breakdown policies emerged as a response to provide specialty coverage for steam boilers. Standard ISO property policy language excludes equipment breakdown caused by artificially generated electrical current, explosion of steam boilers, mechanical breakdown, and other equipment. However, many of these policies pay for the resulting fire. Many times, this critical insurance policy makes the difference between reopening after a loss or going out of business. Equipment Breakdown policies are similar to the technical equipment and machines used in your facility. If not installed and setup correctly, they will not produce the desired end result. Likewise, Equipment Breakdown policies must be tailored to include the appropriate coverage for each unique policyholder's exposure.

When reviewing proposals that include such coverage, policyholders often question whether manufacturer's warranties and well developed preventative maintenance programs are all we need to keep equipment in working order. However, a manufacturer's warranty and preventative maintenance program typically only address changing fluids, visual inspections, and replacement of worn out parts during a defined time period. Unfortunately, this still leaves a considerably uncontrolled exposure to losses. An Equipment Breakdown policy typically addresses the following:

- **direct damage to your business assets and to your customer's items;**
- **loss of income because of suspension of operations;**
- **extra expenses to expedite ordering new equipment; and,**
- **increased costs to repair due to updates in building ordinances and laws.**

Keep in mind, a service contract addresses maintenance and wear and tear issues. Equipment failures can result from things such as supply line surges, excessive moisture, insulation deterioration, single phase operations, overload conditions, lubrication failure,

improper repairs, foreign material on windings, poor contacts, poor connections, or dropped material. These items frequently cannot be adequately captured in a budget.

Looking back at our hypothetical, an equipment breakdown policy would have covered much of the loss. First, the direct damage to the rooftop air-conditioning unit along with the physical damage to the production unit and surrounding property would have been covered. Next, the potential expenses for temporary repairs, renting a nearby facility, and expediting services would have been covered. Last, the policy would cover loss of income and continuing expenses, in addition to employee's payroll. In order to take advantage of this coverage it is important to keep in mind there are specific enhancements that are needed to be added to the policy, such as coverage of off premise utility services. The purpose of insurance is to transfer the risk to a third party that cannot be financed internally. Take the extra step and design your insurance policy to provide the predictable outcome when unpredictable circumstances occur. ■

Andrew Rowles joined SeibertKeck in 2006 to engage with middle market organizations. Andrew holds several designations in the insurance community and is currently pursuing the Certified Insurance Counselor (CIC) certification. Andrew can be reached at 330.867.3140 or at arowles@seibertkeck.com

# Are Businesses Aware of Social Engineering Schemes?

*By Kerri L. Keller*
*kkeller@brouse.com*

Social engineering schemes are on the rise, but do businesses fully understand what that is? Stated plainly, social engineering "refers to the psychological manipulation of people into performing actions or divulging confidential information."[1] While there are numerous "types" of social engineering schemes, the basic premise is similar to all types of theft and involves lying, cheating, and ultimately stealing. One common scheme today is known as the "business e-mail compromise scheme, or "B.E.C." scheme.[2] This scheme is prevalent and can result in "massive financial losses." In fact, the FBI has even warned about the scheme.[3]

The way this scheme works is remarkably simple in application and with precaution, it can be preventable. What happens typically with a B.E.C. scheme is that a criminal researches a company to learn about the employees. He or she finds out who manages the money, "as well as the protocol necessary to perform wire transfers in that business environment."[4] Once armed with this information, the criminal can defraud a company. This is exactly what happened in *Ameriforge Group, Inc. v. Federal Insurance Co.*, a case that was recently filed in Texas.[5]

In *Ameriforge*, the plaintiff alleged it was the victim of a social engineering scheme that started when a criminal, posing as the company's CEO, sent fraudulent emails to a company employee. The email, which requested a wire transfer, was signed by the criminal using the CEO's name, and it contained a specific order to the employee that the transaction was "very sensitive." It further directed the employee to communicate only through email and also to not speak to anyone about the transaction.

The employee, believing he was receiving strict and confidential instructions from the CEO to process a wire transfer, never mentioned it to anyone and proceeded with the transfer. A few days later, the criminal—posing as the CEO—tried again,

**(Continued on page 4)**

but the employee became suspicious and the second fraud was prevented. In an attempt to recover the initial loss, Ameriforge filed a claim with its insurer, arguing that the loss was covered under the policy's Forgery and Computer Fraud/ Computer Violation coverage provisions.


The insurer denied the claim, in large part, because of the employee's actions in facilitating the fraud.[6] And, from a recent survey of cases dealing with these schemes, it is not unusual. While insurance can cover such losses, insurers are quick to deny these types of claims, especially if an employee is involved (even if such involvement is not intentional). In this case, *Ameriforge* settled before the court could reach the many coverage-related issues; however, the circumstances beg the question of whether it had policies in place that could have prevented the fraud. For instance:

- **Were "front-end" measures in place? Were employees using proper and updated passwords? Was sensitive and confidential information disposed of through shredding, rather than being placed in the regular trash bins? Were visitors allowed free access to places where sensitive information is handled? Was network security strong enough to detect phishing and fraudulent emails aimed at social engineering? Was information stored in the cloud secure?**
- **Were "back-end" measures in place? Were employees required to verbally confirm with someone the authenticity of a wire transfer request? Did wire transfers require approval from more than one person before being sent? Were employees even aware of social engineering, or what it looks like?**

While insurance coverage in this area is changing and new endorsements are becoming available to protect policyholders, the pursuit of coverage for social engineering fraud and similar computer-related crime can present challenges. This area of law is not only newly emerging, it is also presently unsettled. Thus, the best way for businesses to handle this risk is to prevent the loss from happening in the beginning. While all businesses should do their best to ensure proper insurance coverage is in place, the importance of proper preventative measures cannot be overstated. ■

[1]*See generally* https://en.wikipedia.org/wiki/Social_engineering_(security) (last visited 3/9/17).
[2]*See generally* https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/fbi-warns-of-rise-in-schemes-targeting-businesses-and-online-fraud-of-financial-officers-and-individuals (last visited 3/9/17).
[3]*Id.*
[4]*Id.*
[5]*Ameriforge Group, Inc. v. Federal Ins. Co.*, No. 4:16-cv-00377 (S.D. Texas 2016).
[6]*Id.* at Exhibit C, p. 4.

# Does Your D&O Policy Provide Coverage for Government Investigations?

*By Gabrielle T. Kelly*
*gkelly@brouse.com*

Federal and state government agencies are increasingly exercising their authority to conduct extensive investigations and bring enforcement actions. In addition, the question of insurance coverage for fees and costs incurred in connection with governmental inquiries and administrative proceedings has become a frequently litigated issue. Depending on the nature of the investigation and the language of your Directors & Officers (D&O) policy, there may be coverage available.

**Defining "Claim"**

Courts have been conflicted on whether an investigation constitutes a claim under a D&O policy. While the policy definitions of "claim" may differ somewhat, they all tend to provide coverage for a written monetary demand, or a civil, criminal, or administrative demand for non-pecuniary relief. Some courts have held that a governmental subpoena constitutes a claim that is covered under the policy, because the insured was responding to a "formal or informal investigative order" that is the main investigative tool available to the government for determining whether it has a claim against a company. *MBIA Inc. v. Federal Ins. Co.*, 652 F.3d 152, 159 (2d Cir. 2011).

Conversely, other courts have held that a "claim" does not include a mere request for information or an explanation for some adverse result. Specifically, the Sixth Circuit held that a demand for documents is not a demand for relief, and thus did not amount to a "claim" under the insured's policies. *Employers' Fire Ins. Co. v. ProMedica Health Systems, Inc.*, 524 Fed. Appx. 241 (6th Cir.2013).

In *ProMedica*, the Federal Trade Commission (FTC) notified ProMedica that it was conducting an investigation to determine whether the acquisition of another hospital was a violation of antitrust laws. Once the FTC commenced an administrative action against ProMedica, the company notified its insurer of the claim. The insurer denied coverage on the basis that ProMedica had knowledge of a claim once it received the initial letter from the FTC.

The Sixth Circuit overturned the district court's ruling that the investigation was a claim. The Court found that the FTC did not "assert to be true" or "declare" that antitrust violations had occurred, and that there was no claim for relief at the time of the initial notice. *Id.* at 248. Accordingly, there was not a claim until the FTC commenced an action.

**Conclusion**

The differing outcomes in these cases demonstrate that a policyholder should not assume that a government investigation is covered by their D&O policy. If you are called upon to respond to a governmental inquiry, take the following steps:

- **Be familiar with how your insurance policies define "claim;"**
- **Notify your insurer immediately of costs incurred from investigations by government entities; and**
- **Contact experienced insurance coverage counsel to discuss the situation to preserve coverage if a claim is later made.** ■

# Cyber Crime: Pathways to Coverage are Illuminating for Certain Losses

*By P. Wesley Lambert*
*wlambert@brouse.com*

There can no longer be any question that the United States, and the world in general, has seen a substantial uptick in the number and complexity of cyber crimes being committed against businesses of all sizes and industries. Nor can there be any question that everyone is at risk, from the local corner store to the Fortune 500 company employing the most sophisticated of cyber attack defense systems. The FBI's Internet Crime Complaint Center ("IC3") reports that over the last five years, the IC3 has received an average of nearly 300,000 complaints per year.[1]

The proliferation of cyber crimes worldwide has led to an increase in the number of insurance coverage lawsuits filed by and against policyholders looking to their insurance carriers to cover some or all of their incurred losses. As a natural consequence of increased litigation, new law has developed providing guideposts to litigants assessing the strengths and weaknesses of their case.

One of the more important issues confronting policyholders is the extent to which their losses must be a "direct" result of a computer-related crime. Two recent decisions from the past year show how policyholders might address this "directness" requirement when challenged to do so.

In *State Bank of Bellingham v. BancInsure, Inc.*, 823 F.3d 456 (8th Cir. 2016), the Eighth Circuit Court of Appeals affirmed a decision in favor of a policyholder, a small local bank. In *Bellingham*, a bank employee responsible for wiring funds through the Federal Reserve's FedLine system left for the day after completing a wire transfer but without removing two important security "tokens" from her computer or shutting the computer down. *Id.* at 457. The next morning, she returned to work to discover that two unauthorized transfers had been executed from

[1]https://pdf.ic3.gov/2015_IC3Report.pdf

Bellingham's account to two different foreign banks. A subsequent investigation revealed that the subject computer had been infected with a "Zeus Trojan Horse." This virus, at the opportune time, permitted unauthorized access to the infected computer for the fraudsters to effectuate the unauthorized wire transfers. *Id.* at 457-58.

Bellingham then looked to BancInsure and the financial institution bond it issued for recovery. After finding that the bond was the equivalent of an insurance policy under Minnesota law, and rejecting several of the insurer's other arguments, the Eighth Circuit found that the unlawful computer hacking by a third-party was the "efficient proximate cause" of the policyholder's loss. *Id.* at 461. The court affirmed the district court's rejection of the insurer's argument that the policyholder's employee's failure to adhere to security protocols was the overriding cause of the loss. Instead, as the Eight Circuit noted that even if the employee's negligent actions "played an essential role" in the loss and created a risk of intrusion into the bank's computer system, "the intrusion and the ensuing loss of bank funds was not 'certain' or inevitable." The 'overriding cause' of the loss Bellingham suffered remains the criminal activity of a third party." *Id.*

The Northern District of Georgia's decision in *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*, No. 15-cv-4130, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016) also represents a policyholder victory, entitling the policyholder to coverage for a $1.7 million loss resulting from a social engineering fraud scheme. In *Principle Solutions*, an employee of the policyholder received a fraudulent email purporting to be from one of the company's managing directors and directing the employee to discretely wire funds to an account for company acquisition. The employee subsequently received phone calls from an individual posing as the company's attorney who coaxed the employee into wiring $1.7 million to a fraudulent account. *Id.* at **1-2.

Principle sought coverage under its commercial crime policy, which covered losses "resulting directly" from fraudulent instructions to a financial institution. *Id.* at *2. Ironshore argued that the loss did not result "directly" from the fraudulent email because the crime required additional actions by the company employee such as communicating with the financial institution and because the employee voluntarily initiated and completed the wire transfer. *Id.* at *4.

The district court, finding both parties' interpretation of the policy's "resulting directly from" language to be reasonable held that that the provision was ambiguous. As such, the court was compelled to adopt the policyholder's interpretation, providing coverage even where there were intervening events between the fraud and the ultimate loss. *Id.* at *5. It is noteworthy, however, that the court relied upon a similar decision in *Apache Corp. v. Great American Insurance Co.*, 2015 WL 7709584 (S.D. Tex. Aug. 7, 2015). The Apache decision was ultimately reversed by the Fifth Circuit Court of Appeals which found an insufficient nexus between the computer-related fraud and the policyholder's ultimate loss. 662 Fed.Appx. 252 (Oct. 18, 2016).

The recent decisions in *Bellingham and Principle Solutions* show that policyholders may be entitled to coverage for cyber crime-related losses even where other factors were at play that contributed to the loss. While cyber crime cases are highly fact-intensive and can turn on terms specific to the insured's policy, the presence of other contributing causes of a cyber crime loss should not automatically deter the policyholder from seeking coverage. ■

## Office Locations

### Akron
388 South Main Street, Suite 500
Akron, OH 44311-4407
Phone: 330.535.5711

### Cleveland
600 Superior Avenue East, Suite 1600
Cleveland, OH 44114-2604
Phone: 216.830.6830

### Youngstown
6550 Seville Drive, Suite B
Canfield, Ohio 44406-9138
Phone: 330.533.6195

### Lorain County
5321 Meadow Lane Court, Suite 7
Sheffield Village, OH 44035-0601
Phone: 440.934.8080

### Insurance Recovery Attorneys
Lucas M. Blower
Kate M. Bradley
Nicholas P. Capotosto
Christopher J. Carney
Alexandra V. Dattilo
Clair E. Dickinson
Bridget A. Franklin
JoZeff W. Gebolys
Matthew K. Grashoff
Kerri L. Keller
Gabrielle T. Kelly
P. Wesley Lambert
Amanda M. Leffler
Sallie Conley Lux
Caroline L. Marks
Meagan L. Moore
Amanda P. Parker
Paul A. Rose
David Sporar
Christopher T. Teodosio
Anastasia J. Wade

# Attorney Highlights

**Amanda M. Leffler** and **Caroline L. Marks** were recently appointed co-chairs of the Insurance Recovery Practice Group.

**Amanda M. Leffler** spoke on Additional Insured Coverage at the American Bar Association Section of Litigation, Insurance Coverage Litigation Conference on March 3, 2017.

**Amanda M. Leffler** and **Lucas M. Blower** spoke at the Environmental Forum with co-sponsors SeibertKeck Insurance, SandRun Risk and EnviroScience, Inc.

**P. Wesley Lambert** was appointed as a co-chair of the Employment Committee for the Insurance Coverage Litigation section of the American Bar Association.

**Matthew K. Grashoff** was selected for the Ohio State Bar Association Leadership Academy, a state-wide program intended to foster leadership skills and provide professional development opportunities to lawyers recently admitted to practice.

Earlier this year, ATHENA Akron honored **Bridget A. Franklin** and **Kerri L. Keller** at a reception to honor established women leaders who are new to their positions. Ms. Franklin was recently elected to the position of shareholder at Brouse McDowell, and Ms. Keller was named co-chair of the firm's Litigation Practice Group.

*Register Now at seminars@brouse.com*

**Cyber Crime Breakfast Briefing**
How to Protect Your Business from Cyber Risks
Presented by Brouse McDowell & Maconachy Stradley
**Thursday, May 11, 2017**

**Breakfast & Registration 8:00 a.m. – 8:30 a.m.**
**Presentation 8:30 a.m. – 9:30 a.m.**
**Location:**
U.S. Acute Care Solutions (USACS) of Canton
4565 Dressler Rd. NW
Canton, Ohio 44718