

CYBER & EMPLOYMENT STRATEGIES TO PROTECT YOUR BUSINESS



THURSDAY, FEBRUARY 28, 2019
Nationwide Hotel & Conference Center



Mazanec, Raskin & Ryder Co., L.P.A.

Attorneys and Counsellors at Law



Agenda



- Welcome/Opening Remarks
- #MeToo
- Workplace Safety
- Break
- Cyber Security
- Lunch
- Panel: Cyber Strategies


February 28, 2019

Mazanec, Raskin & Ryder Co., L.P.A.
Attorneys and Counsellors at Law

#YouToo: The Impact of #MeToo on Sexual Harassment Claims

Tami Z. Hannon
Partner

February 28, 2019

Mazanec, Raskin & Ryder Co., L.P.A.
Attorneys and Counsellors at Law

HISTORY OF #METOO



#HERTOO



BY THE NUMBERS

- Facebook reports that 45% of users had a friend that posted #MeToo.
- Percent of women that report being harassed?
 - Most comprehensive study
 - Restaurant environments
 - Legal profession
- Percent of men that reported hearing sexist comments?
- Percent of women that report harassment internally?

BY THE NUMBERS

- **Harassment**
 - 28% reported unwanted sexual advances
 - 50 – 60% of harassment concerned making inappropriate comments or trying to discuss sex
 - 50% report occurring 5 or more times

Employee complained a male coworker made sexual jokes and comments, and showed sexually inappropriate pictures to her and other female employees. Employee reported the events, but the employer failed to respond. When left unchecked, the behavior escalated to unwanted touching. The employee continued to complain and was subjected to what she perceived as retaliation. After sending an email to corporate office complaining of her treatment, she was fired.

Jury awarded \$300,000 in compensatory damages and \$1.75 million in punitive damages.

JURY AWARDS

- **March 2, 2018 - \$13.4 million awarded by New York jury against Domino's Sugar**
 - \$11.7 million represented punitive damages
- **March 8, 2018 - \$2.6 million awarded by California jury**
 - "We're glad it didn't happen to a woman."
- **August 2018 – "I love Latina women."**
- **September 2018 - \$7 million to former Attica teacher**
- **November 14, 2017 - \$1 verdict against university researcher**
 - \$300,000 attorney's fees
 - "Preventing sexual harassment to enable broad participation of all genders in the workforce is an important public goal."

- **July 27, 2018 - \$1.25 million awarded by New York Jury against Columbia University Business School**
- **EEOC Settlements**
- **Derivative Suits**
 - Wynn Resorts – Jan. 26, 2018
 - Twenty First Century Fox – April 2018
 - CBS – Aug. 27, 2018
 - Nike – Aug. 28, 2018
 - Papa John's International – Aug. 30, 2018
 - Google – January 11, 2019

WHAT DOES THIS MEAN FOR EMPLOYERS?

- **Americans favor zero tolerance of sexual harassment**
 - 78% of women now say that they are more likely to speak up
 - 77% of men now say that they are more likely to speak up
- **Jury Make-up**
 - Typical jury – 8 people, about half women
 - 40-60% - 2 women who have been harassed
 - 45% - 4 who know someone that has been harassed

WHAT DO JURIES EXPECT?

- **Fair procedures to uncover the truth**
 - Accessible reporting methods
- **Employee to be placed on leave or at least separated**
- **Investigation**
- **Standard credibility evaluation**
- **Appropriate discipline**
 - Not automatic termination
 - Discipline of all employees involved
- **Policy**
- **Training of employees**

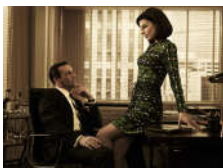
POLICY EXPECTATIONS

- Clear and simple explanation of conduct with examples
- Retaliation protections
- Clear process with multiple reporting avenues
- Assurances of confidentiality
- Process for prompt, thorough and impartial investigation
- Prompt and proportionate corrective action
- Respond to behavior that can rise to level of harassment if left unchecked

INVESTIGATIONS

- Who do you interview?
- Confidentiality?
- What do you ask?
- Reviewing what you found
- Standard to apply
- Documentation
 - Finishing Steps
 - Storage

CULTURAL SHIFT



Powerful Men
Vs.
Work should be about work.



TRAINING

- 2016 EEOC Study
- What topics do you cover?
- How to train
- How often to train
- Documentation

Tami Z. Hannon

100 Franklin's Row
34305 Solon Road
Cleveland, OH 44139
P:440.424.0009
F:440.248.8861
thannon@mrirlaw.com



CYBER & EMPLOYMENT STRATEGIES TO PROTECT YOUR BUSINESS



THURSDAY, FEBRUARY 28, 2019
Nationwide Hotel & Conference Center

WORKPLACE SAFETY

Stacy V. Pollock
Partner

February 28, 2019



Mazanec, Raskin & Ryder Co., L.P.A.
Attorneys and Counselors at Law



Mazanec, Raskin & Ryder Co., L.P.A.
Attorneys and Counselors at Law

DUTY TO PROVIDE SAFE ENVIRONMENT

- No employer shall maintain any place that is not safe. R.C. § 4101.12.
- No employee shall take any action that makes a place of business unsafe. R.C. § 4101.12.



Mazanec, Raskin & Ryder Co., L.P.A.
Attorneys and Counselors at Law

- What does “safe” mean?
 - Means a condition or premises that does not pose a danger to a person’s mental or physical health.
 - Truly safe workplaces are unattainable.
- How far does an employer have to go to ensure that safety before it has met its duty under the law?
 - Have to reasonably respond to threats and potential threats to safety.
 - Have to comply with industry standards/legal standards pertaining to safety.

EMPLOYER LIABILITY: CIVIL LIABILITY

- ***Negligence Claims***—employers that comply with the Ohio Workers' Comp Act are not liable for work-related injuries, illness or deaths caused by negligence in the workplace.
- ***Intentional Torts***—(1) employer's knowledge of the dangerous condition, (2) employer's knowledge that harm is a substantial certainty, and (3) with this knowledge, the employer required the employee to perform the dangerous task.

EMPLOYER LIABILITY: OSHA/VSSR CLAIMS

- ***Occupational Safety and Health Administration***—The Federal Government's watchdog on private employers to ensure that they provide reasonably safe working conditions. Requires employers to comply with a number of requirements, and provides a mechanism for employees to report conditions that threaten safety.
- ***Violation of Specific Safety Rule***—An Injured Worker with a BWC claim may be eligible to receive an additional award of compensation if the injury occurred as a result of the employer's violation of a specific safety requirement.

ANTI-RETALIATION BEST PRACTICES:

1. Provide thorough training to all employees.
2. Adopt safety rules that are specific and clear.
3. Incorporate the disciplinary policy into the safety program.
4. Clearly communicate to the employee what he/she did wrong.
5. Use progressive discipline as appropriate.
6. Document your investigation and the outcome of the investigation.
7. Equally enforce the safety rules.

EMPLOYEE REFUSAL TO WORK BECAUSE OF SAFETY ISSUES

1. Employee complained to the employer about the dangerous condition and the employer refused to correct it;
2. A reasonable person in the employee's position would agree that there's an immediate danger of death or serious injury; and
3. Because of the urgency, there is no time to wait for the unsafe condition to be corrected through proper channels (ie. OSHA, Union grievance, policy grievance).

KEY TERMS FOR WORKPLACE SAFETY POLICIES:

- Statement that employer is committed to ensuring safety of all individuals.
- Mandatory immediate reporting of all accidents involving injury, no matter how minor the injury, or risk of serious injury.
- Consistent incident report form with clear direction on who the report is to be submitted to and by when (no more than 24 hours).
- Encourages employees to report workplace safety concerns to specific individual responsible for employer's safety.

EMPLOYEE PERFORMANCE EVALUATIONS

- Does it make sense to put safety evals into annual performance evals?
- Prepare safety evals in a way that triggers a re-training requirement if certain standards are not met.
- Supervisor safety evals must take safety to the next level.

DISCIPLINING EMPLOYEES FOR WORKPLACE SAFETY VIOLATIONS

- Avoid practices which encourage non-reporting of violations.
- Is retraining more appropriate than discipline?
- Avoid retaliation claims by enforcing clearly defined policies.

PRESCRIPTION DRUGS AND WORKPLACE SAFETY

- ADA does not protect against individuals currently using illegal drugs.
- Policies should make clear that employees in safety-sensitive positions have an ongoing duty to report all prescription and non-prescription drug use that may affect their job performance.
- Policies should not have a blanket prohibition of legal drug use.
- Request a medical certification for employees who test positive for prescription drugs.

WORKPLACE VIOLENCE

Three Keys to Prevention:

- **Policy**
 - Definition of violence (including verbal violence)
 - Process of immediate removal and investigation
 - Mandated reporting of suspicions
- **Communication—early intervention is critical**
- **Training**

CONCLUSION

- Duty to maintain safe work environment;
- Duty to avoid retaliation claims by employees;
- Duty to maintain effective safety policies;
- Duty to evaluate employee safety practices;
- Duty to appropriately monitor employee drug use; and
- Duty to institute practices to prevent workplace violence.

Stacy V. Pollock

175 South Third Street
Suite 1000
Columbus, OH 42315
P: 614.324.0163
spollock@mrlaw.com



CYBER & EMPLOYMENT STRATEGIES TO PROTECT YOUR BUSINESS



THURSDAY, FEBRUARY 28, 2019
Nationwide Hotel & Conference Center

CYBERSECURITY EURO-STYLE

THE GDPR AND THE US RESPONSE

Barry Miller
Partner

Chenee Castruita
Associate

February 28, 2019



Mazanec, Raskin & Ryder Co., L.P.A.
Attorneys and Counselors at Law



Mazanec, Raskin & Ryder Co., L.P.A.
Attorneys and Counselors at Law

WHAT IS THE GDPR

- **General Data Protection Rule**
 - a/k/a Regulation (EU) 2016/679
- **Single standard for data controllers and processors**
- **Focuses on protection of data and breach notification**



Mazanec, Raskin & Ryder Co., L.P.A.
Attorneys and Counselors at Law

CURRENT US APPROACH

- **Ad hoc**
 - Federal agencies govern data in their area
 - HHS governs HIPAA (OCR enforces)
 - FTC governs banking and credit
- **States' focus – breach notification**
 - All 50 states now have notification laws

CURRENT US APPROACH (OHIO)

- **Ohio statute passed in June, effective Nov. 2**
 - Safe harbor defense in suits for data breach
 - Defense available if the business creates a plan that “reasonably conforms” to one of eight cybersecurity frameworks
 - NIST Cybersecurity Framework
 - Security requirements of HIPAA, HI-TECH, etc.

CURRENT US APPROACH

- **Who owns the data?**
 - Data aggregators believe they own it
- **Is there any such thing as too much data?**
 - Most aggregators think not
- **What can I do with the data?**
 - Most aggregators think anything short of disclosure

GDPR v. US APPROACH

- **Single-source comprehensive data regulation**
- **The “data subject” owns the data**
 - And mostly controls how the data can be used, having the ability to withdraw consent
- **“Privacy by design” (as little data as possible)**
- **Opt-in to processing v. Opt-out**
- **Breach prevention emphasized**

DO I HAVE TO WORRY ABOUT THE GDPR

- **Applies to data processors/controllers**
 - Who provide “goods and services”
 - Who collect “personal data” of a EU resident, OR of a person who is in the EU at the time of collection, regardless of whether data is held or processed in EU



GLOBAL ENGAGEMENT NEWS
Check out the newsletter to stay updated on Global Engagement's activities on campus and in Columbus.

INTERNATIONAL STUDENTS

You are here: [Home](#) • [Exchange Students](#)

APPLICATION INSTRUCTIONS


INTERNATIONAL PARTNERSHIPS

EXCHANGE PARTNER PROGRAM

THE OHIO STATE UNIVERSITY INTERNATIONAL EXCHANGE PROGRAM (IEP)

The J-1 exchange visitor program was developed in 1951 by an act of Congress and is administered by the U.S. Department of State, with its main goal to "increase mutual understanding between the people of the United States and the people of other countries by means of educational and cultural exchanges."

[Exchange students are admitted in a non-degree status at the undergraduate or graduate level to attend Ohio State for autumn semester, spring semester, or both autumn and spring semesters. Students are expected to return to their home university after the completion of their exchange study.]





Mazanec, Raskin & Ryder Co., L.P.A.
Attorneys and Counselors at Law

METRO NEWS

U.S. colleges see decline in foreign students, but Ohio State expects increase

Updated Sep 11, 2018; Posted Sep 10, 2018



DO I HAVE TO WORRY ABOUT THE GDPR

• Personal Data

- Any information relating to an identified or identifiable natural person.
- A name, ID number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.



"...we collect Personal Information consisting of, at a minimum, your name, email address, mobile phone number, vehicle license tag number and issuing jurisdiction, Payment Method, Payment Information, Username and password."



Sign In / Sign Up

2. How We Collect Information and What We Collect

When you open an account with us whether by downloading and installing the App, registering on our Site, using our GPS System, or contacting Member Services, we collect Personal Information consisting of, at a minimum, your name, email address, mobile phone number, vehicle license tag number and issuing jurisdiction, Payment Method, Payment Information, Username and password.

—Over the course of your use of the Platform, we may collect additional Personal Information such as your mobile, address, billing address, Transaction data, GPS data, information that you voluntarily provide Member Services. Information received from your credit card payments (digital wallet) or financial institution information necessary to address your bill requests or to troubleshoot problems information provided in connection with your membership (card information) compliance and communication you have with us and your statements and payment.

We and our service providers use Cookies and other technologies (e.g., Web Beacons, JavaScript tags, and web beacons) to collect information about your use of the Platform and on our Site and information about the device you use to access the Platform, such as your Mobile Device's unique identifier, address, operating system, manufacturer, screen resolution, operating system name and version, device manufacturer, network carrier, Internet Service Provider, browser type and version, the name and version of the Platform you are using, traffic data, device and usage data, etc.

We do not collect sensitive information (information that you have or are entitled to, or that is otherwise protected by law), or information that is subject to special protection under applicable law, such as race, ethnicity, gender, sexual orientation, or other sensitive information. We may use or share such information with third parties for any lawful purpose.

DO I HAVE TO WORRY ABOUT THE GDPR

- **Requires those covered to “implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation.”**
 - In other words: “have a data protection plan.”

DO I HAVE TO WORRY ABOUT THE GDPR

- Requires those covered to “implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation.”
 - In other words: “have a data protection plan.”
 - And your plan better include third party vendors.

REVIEW

- Do you actively market goods or services in the EU, and collect data from EU residents?
- Do you have a client who actively markets goods or services in the EU, and collects data from EU residents?
- Might you ever collect data from an EU resident?

If any of these answers is “yes,” then Europe thinks you should worry about the GDPR.

GDPR: Google and Facebook face up to \$9.3B in fines on first day of new privacy law

An Austrian privacy group is waiting no time.

Google fined €50 million for GDPR violation in France

The CNIL, said Google's data company profiles aren't easily accessible or transparent.

How to avoid pulling a Google and copping a \$80 million fine for data misuse

NICHOLAS BLACKMORE | Monday, February 18, 2016

CALIFORNIA CONSUMER PRIVACY ACT (2018)

- **Tracks the EU GDPR in many ways, including:**
 - A broader definition of “personal data” than is in general use in the US
 - Requiring businesses to implement opt-in rather than opt-out for their consumers

NY DFS CYBERSECURITY REGULATION (2017)

- **Banks, insurers, and other financial service providers doing business in NY**
- **Imposes minimum standards for**
 - Data protection and encryption
 - Access controls
 - Penetration testing
 - Funding your cybersecurity program
 - Preparing incident response plans

NY DFS CYBERSECURITY REGULATION (2017)

- **Requirements re Third Party Vendors (TPVs)**
 - Assess cyber risks of all TPVs
 - TPVs must meet minimum cybersecurity standards
 - Due diligence in evaluating TPV cyber practices
 - Regular continued assessment of TPV readiness

REVIEW

- Do you do business with EU residents, financial institutions in New York, or with California residents?
- Do you do business with someone who does business in these jurisdictions? Each of them reaches third party vendors.
- Do you do business with someone who does business with someone who does business...?

US PUSHBACK?

- **US Chamber Privacy Principles (Sept. 6, 2018)**
 - Calls for a “Nationwide Privacy Framework” that pre-empts state law
 - Relates privacy protections to “benefits provided and risks presented” by data
 - Encourages “Privacy Innovation”
 - Encourages “Flexibility” in privacy law/regulation

US PUSHBACK?

- **Chamber principles do not address:**
 - Who owns the data?
 - Opt-in v. opt-out
 - Can consent be withdrawn?

SO WHERE DOES THAT LEAVE ME?


- **No clear appetite to support Chamber approach**
- **European approach, as reflected in New York and California, appears to be gaining steam**
- **European approach encourages many things that are part of a good data security plan**
 - Especially in Ohio, under the Safe Harbor Law
 - Implementing such a plan will likely comply with any law based on the Chamber principles

SO WHERE DOES THAT LEAVE ME?


- **Time to start thinking about your data plan**
 - What data you need?
 - What data you need to keep?
 - Where your data is kept?
 - Is your data encrypted?
 - Who can access your data?
 - What do you do if your data is breached?




N. Hanacek/NIST



Mazanec, Raskin & Ryder Co., L.P.A.
Attorneys and Counsellors at Law




Chenee M. Castruita
 175 South Third Street
 Suite 1000
 Columbus, OH 42315
 614.324.1039
ccastruita@mrrlaw.com




Barry Miller
 230 Lexington Green Circle
 Suite 605
 Lexington, KY 40503
 859.899.8513
bmiller@mrrlaw.com

**CYBER & EMPLOYMENT
STRATEGIES TO
PROTECT YOUR BUSINESS**



THURSDAY, FEBRUARY 28, 2019
 Nationwide Hotel & Conference Center



Mazanec, Raskin & Ryder Co., L.P.A.
Attorneys and Counsellors at Law

**CYBER & EMPLOYMENT
STRATEGIES TO
PROTECT YOUR BUSINESS**



THURSDAY, FEBRUARY 28, 2019
 Nationwide Hotel & Conference Center

Workplace Safety

I. What are everyone's duties in workplace safety?

A. Employer's Duty to Provide Safe Environment

1. No employer shall require, permit, or suffer any employee to go or be in any employment or place of employment which is not safe;
2. No employer shall fail to furnish, provide and use safety devices and safeguards, or fail to obey and follow orders or to adopt and use methods and processes reasonably adequate to render such employment and employment and place of employment safe;
3. No employer shall fail to do every other thing reasonably necessary to protect the life, health, safety and welfare of employees or frequenters of the employer; and
4. No such employer or other person shall construct, occupy or maintain any place of employment that is not safe. R.C. § 4101.12

B. Employees' duty to maintain a safe environment

1. No employee shall remove, displace, damage, destroy, interfere with, or carry off any safety device or safeguard furnished or provided for use in any employment or place of employment;
2. No employee shall interfere with the use of any method or process adopted for the protection of any employee or frequenters of the place of business; and
3. No employee shall fail to follow and obey orders and to do every other thing reasonably necessary to protect the life, health, safety and welfare of employee and frequenters of the place of business. R.C. § 4101.13

II. When may an employee refuse to work because of safety concerns?

- A. Employee complained to the employer about the dangerous condition and employer refused to correct it;
- B. A reasonable person in the employee's position would agree that there's an immediate danger of death or serious injury; and
- C. Because of the urgency, there is no time to wait for the unsafe condition to be corrected through proper channels (i.e. reporting to OSHA)

III. What kind of liability are employers to expose to for not maintaining a safe work place?

A. Negligence claims

1. Employers who comply with the Ohio Workers' Compensation Act (including paying all premiums) are not liable for a work-related injury, illness or death. R.C. § 4123.74
2. Settlement agreements in which the employee agrees to not file for workers' compensation in exchange for consideration is not enforceable. Employees cannot waive their right to file for workers' compensation benefits.

B. Intentional torts

1. Elements

- a. Employer's knowledge of the existence of a dangerous process, procedure, instrumentality or condition within its business operation;
- b. Employer's knowledge that if the employee is subjected by his employment to such dangerous process, procedure, instrumentality or condition, then harm to the employee will be a substantial certainty; and
- c. The employer nevertheless required the employee to continue to perform the dangerous task.

2. Employer's knowledge that asbestos existed at its manufacturing facility, and that exposure to asbestos could lead to injury, was not sufficient to show that employer knew that harm to employee as a result of asbestos exposure would be a substantial certainty, as an element of claim of employer intentional tort by employee who was diagnosed with mesothelioma, allegedly caused by asbestos exposure; employer complied with all safety regulations in force at time of employee's exposure, methods and materials employer used at time of exposure were state of the art for the times, and employee testified that he believed that employer was concerned about worker safety and that employer had provided safety equipment. *Fagerholm v. Gen. Elec. Co., Inc.*, 2009-Ohio-2390 (8th Dist.)

C. Violation of Specific Safety Rule (VSSR) Claims

1. An injured worker with a BWC claim may be eligible to receive an additional award of compensation if the injury occurred as a result of the employer's violation of a specific safety requirement.

2. Industry standards and OSHA laws may be considered by the Industrial Commission in interpreting the VSSR regulations.

- a. An employee was injured when he fell from a 14 foot ladder while working on a billboard. The Ohio Administrative Code (OAC) requires employers to provide safety harnesses and lanyard, and employees must wear them, when working more than 6 feet above ground. The OAC requires employees to fasten the safety devices “to the structure.” The Injured Worker attached the lanyard to the ladder instead of to the billboard and fell. The Injured Worker filed a VSSR claim, alleging the employer unlawfully trained him to attach the lanyard to the ladder. The Industrial Commission denied the VSSR claim because the OSHA regulations and industry standards state that once the ladder’s hooks are secured properly to the structure, the ladder becomes a part of the structure. It is therefore in compliance with the OAC to clip into the ladder once the ladder is hooked to the structure. The Ohio Supreme Court held that it was proper for the Industrial Commission to look to the OSHA regulations and industry standards to define the OAC’s meaning of “the structure.” *State ex rel. Richmond v. Indust. Comm.*, 139 Ohio St.3d 157 (2014)
- b. The Industrial Commission will look to the egregiousness of the violation, the employer’s safety records and the severity/extent of the employee’s injury.
- c. An employee’s own negligence is not a defense to a VSSR claim if the employer did not comply with the applicable safety regulation. *Armstrong Steel Erectors, Inc. v. Indust. Comm.*, 144 Ohio St.3d 243 (2015)

3. Penalties

- a. Additional award is purely punitive and ranges from 15% to 50% of the maximum allowable weekly compensation granted to the Injured Worker.
- b. Civil penalty of up to \$50,000 against an employer with two or more safety violations in a 24 month period.

4. VSSR Process

- a. Claim is allowed by BWC
- b. Injured worker will file an IC-8/9 form within 2 years of the injury, death, disease diagnosis

- c. Industrial Commission notifies all parties of the filing
 - d. BWC investigates (inspection of site, interviews, document review)
 - e. Investigator files a Report of Investigation with Industrial Commission
 - f. Parties receive the Report and have 30 days to supplement the report
 - g. Industrial Commission schedules a pre-hearing conference to discuss new information, possible settlement, set hearing date
 - h. Merit hearing scheduled and held. The Injured Worker has the burden to show that the safety requirement was both specific and applicable, the employer was not in compliance when the accident occurred, and the non-compliance contributed to the injury, illness or death.
 - i. Industrial Commission may grant an additional award and issue a correction order
 - j. Investigator will ensure that the Employer complied with the correction order
5. Employer liability under OSHA (Occupational Safety and Health Administration)
- a. Employer must prominently display OSHA Rights and Responsibilities Poster
 - b. Inform workers about chemical hazards through training, labels, alarms, color-coded systems, chemical information sheets and other methods
 - c. Provide safety training to workers in a language/vocabulary they can understand
 - d. Keep accurate records of work-related injuries and illnesses
 - e. Perform tests in the workplace, such as sampling, as required by some OSHA standards
 - f. Provide required personal protective equipment at no cost to workers

- g. Provide hearing tests or other medical tests required by OSHA standards
 - h. Post OSHA citations and injury and illness data where employees can see them
 - i. Notify OSHA within 8 hours of a workplace fatality or within 24 hours of any work-related in-patient hospitalization, amputation or loss of an eye
 - j. Do not retaliate against workers exercising their rights, including their right to report a work-related injury or illness
- 6. Retaliation liability
 - a. Retaliation laws
 - 1.) Employers shall not retaliate against an employee who reports a violation of the law (Ohio Whistleblower's Law). R.C. §4113.52
 - 2.) Employer shall not retaliate against an employee for filing, pursuing, or participating in a workers' compensation claim. R.C. § 4123.90
 - 3.) Exception to at-will employment—terminating employees because they file a workplace safety rule complaint is against public policy.
- 7. Best practices to avoid retaliation claims
 - a. Provide thorough safety training to all employees
 - b. Adopt safety rules that are specific, clear and follow OSHA guidelines
 - c. Incorporate the disciplinary policy into the safety program
 - d. Clearly communicate to employee what they did wrong
 - e. Use progressive discipline as appropriate
 - f. Document your investigation and the outcome
 - g. Equally enforce the safety rules

- IV. What are the benefits of addressing workplace safety in employment handbooks/policies?
- A. Clear policies assist in defending against retaliation claims.
 - B. Policies give supervisors and employees direction.
 - C. Policies show the employer's dedication to safety practices, which mitigates against a VSSR claim.
 - D. Policies encourage employees to report safety practices.
- V. Should employers incorporate workplace safety into performance evaluations?
- A. Safety assessments in performance evaluations is a way to reduce liability.
 - B. Utilize numerical safety evaluations. If an employee falls below a specific number, they are required to be retraining on a safety system.
 - C. Frequency of the evaluation is just as important as the content of the evaluation.
 - D. Sample questions for safety evaluations in performance evaluations of employees:
 - 1. Demonstrates knowledge of the safety responsibilities of the job.
 - 2. Effectively carries out the safety responsibilities (i.e. wearing safety equipment).
 - 3. Maintains/inspects all equipment for safe, operable condition.
 - 4. Completes accident/incident reports in a timely and factual manner.
 - 5. Actively pursues the correction of any safety hazards or violations that he/she is aware of or should be aware of
 - E. Sample questions for safety evaluations in performance evaluations of supervisors:
 - 1. Explains and demonstrates safety in a positive manner.
 - 2. Monitors the safe work habits of new employees.
 - 3. Observes others to ensure safety practices are followed.
 - 4. Exhibits knowledge of the value of equipment safeguards, and assures that they are properly provided, maintained and used.
 - 5. Takes the initiative to inform management of ideas for safer practices.

6. Keeps equipment in top performance and safe condition.
 7. Addresses safety violations or hazards immediately.
 8. Completes accident/incident reports in a timely and factual manner.
- V. What considerations should employers make in disciplining employees for a workplace safety violation?
- A. Is (re)training more appropriate than discipline? What gave rise to the infraction? A willful violation, a momentary lapse in judgment or misunderstanding of the rules?
 - B. Retaliation concerns if the employee is injured
 1. Rebut retaliation concerns by having a clearly defined policy that was communicated to employees.
 2. Be consistent in the enforcement of policies and the severity of discipline.
 - C. Document all discipline, even verbal counseling.
 - D. Discipline may encourage non-reporting of violations.
 1. Supervisors are the best defense against non-reporting of safety violations. Supervisors must be aware of the critical importance of reporting violations, and supervisors must be disciplined if it is discovered that non-reporting is encouraged/occurring.
 2. OSHA inspectors have been looking out for practices which may discourage reporting of violations, such as a bonuses to employees for X period of time without a workplace injury.
 - a. What about a bonus for attending additional safety training?
 - C. Industrial Commission's wage loss eligibility for terminated employees—The question is whether the employee voluntarily abandoned employment (and thus is not eligible for wage loss benefits) because he/she violated a work rule.
 1. If an employee's departure from the workplace was causally related to the injury, it does not preclude the employee's eligibility for temporary total disability (TTD) compensation. *Gross v. Indust. Comm.* 115 Ohio St.3d 249 (2007)
 2. But, if the decision had been made prior to the industrial injury and the Industrial Commission can be certain that the Injured Worker would not

continue to be employed even if he/she had not been injured, then TTD is not appropriate. *Sheets v. Indust. Comm.*, 2017-Ohio-1169 (10th Dist.)

3. In order to terminate an employee for a violation of a workplace rule, the following elements must be met for the Industrial Commission to deny wage loss compensation:
 - a. Conduct must be clearly prohibited;
 - b. The conduct must be previously clearly defined as a dischargeable offense; and
 - c. The Injured Worker knew or should have known that the conduct was prohibited and could lead to termination. *State ex rel. Louisiana-Pacific Corp. v. Indust. Commn.* 72 Ohio St.3d 401 (1995)

Ransomware *on the Rise*

by Barry Miller and Curt Graham, Mazanec, Raskin & Ryder Co., LPA

The message on your computer seems friendly — almost as if it were offering help. “Your data has been encrypted,” it says. “But don’t worry; it can be decrypted. All you need is a decryption key, which we are happy to sell you.”

That message means the computer has been infected by ransomware, a type of software attack that is decidedly unfriendly, as it holds the user’s data hostage for ransom. Users across the country have learned that the intent behind the message is anything but friendly. That includes local governments. Kentucky cities can take warning from their counterparts in other states, especially Ohio, which has been particularly hard hit in the past few years:

- In January, all government offices in Licking County, Ohio — 1,000 computers and a dozen servers — were shut down for nearly two weeks while the county determined whether it would pay the \$31,000 ransom hackers demanded. The county ultimately decided that its backups were sufficient to rebuild its electronic records, which it did at the cost of more than \$50,000 (\$25,000 of which the county paid as a deductible on its cyber insurance policy).
- In April 2016, a fiscal officer in Vernon Township opened an email that was made to look like one from a shipping company. When she opened the email, the ransomware installed itself. The program demanded \$200 for a decryption key, but because the township had good backups, it was able to restore the data.
- In October 2016, a ransomware attack affected as many as 17,000 voter records in Henry County, Ohio.
- A county court in eastern Ohio paid a \$2,500 ransom to unlock its data because it did not have usable backups.

Kentucky is not immune to this alarming trend. In March, Methodist Hospital in Henderson declared itself in a state of emergency after an attack lasting five days. The hospital resolved the situation without paying hackers, but according to Mike Sunseri, deputy director of the Kentucky Office of Homeland Security, that experience may be an exception. “The bottom line is that these kinds of attacks are going to become more common because people are paying the ransom,” Sunseri said.

He also related that a chain of hospitals in Kentucky, Virginia and West Virginia sustained ransomware attacks last year that left some of them resorting to pen and paper to do their work, reducing effectiveness to 20 percent.

Ransomware has evolved from spam attacks, broadcast to a large number of users, demanding \$200 to \$300. Many ransomware attacks

are more targeted now and also demand more money. Hospitals were a logical target for such attacks because of the kind of work they do and their dependence on computer systems holding patient data. “There is a sense of urgency when lives are on the line,” Sunseri said.

Because they hold sensitive information in their computer systems, and because they provide critical services, city governments and other local agencies are also logical targets for such attacks. “How long can your fire department be down?” asked Dave Mims, CEO and founder of Sophicity, an information technology company that partners with the Kentucky League of Cities. “How long can a city continue to offer electric service if it can’t send out its utility bills?”

Because of budget constraints, local governments (especially smaller ones) may depend on legacy computer systems, which are more susceptible to all types of cyberattacks, including ransomware. The WannaCry Ransomware attack, first reported on May 12, 2017, affected more than 300,000 computers by the end of that month. That malware was built to take advantage of a vulnerability in older Windows operating systems.

How Does Ransomware Work?

Ransomware is most commonly distributed by emails that try to induce readers to click on a link — such as the “shipping” email sent to the Vernon Township fiscal officer. The type of deceit often depends on the season. Emails from purported shipping companies or retailers will often hit during the Christmas holidays. Others claiming to be from the Internal Revenue Service or accountants are prevalent in the weeks before April 15.

A user who clicks on a link or opens an attachment from one of these emails causes the download of an exploit kit, which installs ransomware on the affected computer. Once that installation is complete, the user is presented with a screen like the one below (from the WannaCry ransomware), which effectively is the ransom note.

This screen demands a \$300 payment for the decryption key. A typical feature of ransom screens is the countdown, as shown on the left-hand side of the pictured screen. It tells the victim when the initial demand will double after the countdown expires. A second countdown tells the victim when the files will be locked forever.



Ransomware is a program loaded on victims' computers via a phishing email or by exploiting vulnerabilities in the computer's operating system. Once loaded and executed, the ransomware encodes files on the affected computer, locking them from use. The data can only be made readable again by using the correct decryption key. The ransomware will also try to propagate itself onto networks to which an affected computer connects.

One logistical issue is that the demand usually requires payment in Bitcoin, an untraceable digital currency that is not backed by any government or central bank. A victim who decides to pay the ransom must figure out how to obtain and transfer Bitcoin.

Who Is Behind Ransomware?

Ransomware programs generally are written by overseas criminal enterprises, most often Russian and Eastern European. Those enterprises sell software kits to would-be extortionists, sometimes for a nominal amount but usually for a price that includes a percentage of the ransom the buyer can harvest. The buyers of the software are responsible for its distribution. The enterprises that sell the software compete on features and even on “customer service” they provide to the victims who download their product. (Some versions of ransomware may even offer a reduced ransom to victims who leave a positive review of their experience.)

In a strange way, the success of ransomware is built on trust — the victims' belief that if they pay the ransom, they actually will receive a key that will decrypt their files and allow the victims to regain access to their data. Because the typical ransom demand is relatively small, the distributors are relying on receiving many such payments, which will not happen if it becomes known that they do not deliver what they promise upon payment.

But there is no guarantee that if you pay the ransom, you will regain access to your data. The perpetrators of WannaCry have been unable to distribute decryption keys fast enough to meet demand. Other ransomware hackers simply never have any intention of returning the data. Even if they do, Mims warned, there is no guarantee the data will be accurate. And Sunseri added that there also is no guarantee that, even if they return your data, hackers won't build a back door into your computer network. So paying ransom is not without risk.

Still, some take that risk because the larger risk of being without access to their data is more worrisome. Sunseri understands that. “Our general position is we never encourage anyone to pay the ransom, but it is always the choice of the individual or organization,” he said.

How Can I Protect Against Ransomware?

Ransomware is most often introduced into a computer or network via email, when a user clicks on a link or opens a document that causes the computer to download malware. But WannaCry illustrates that defending against ransomware attacks is not a matter of adopting a single strategy. While it can be initiated through an email, once within a network, it attacks connected machines without requiring users to open attachments or click links.

So dealing with ransomware involves more than one strategy.

Educate Users

Teach computer users to be very wary of emails that contain links and attachments. Emails claiming that the reader may be the beneficiary from the death of an overseas prince are no longer the concern. Today's phishing emails are more sophisticated and are designed to reach users at times when they may be most susceptible to clicking on a link, such as the Christmas shipping email. Users must be constantly vigilant and should never click a link or open an attachment if there is the slightest doubt about where the email came from or without verifying the sender's email address.

Bitcoin was created by an anonymous internet user in 2009. This "cryptocurrency" can be used to purchase a variety of goods online, and the number of merchants accepting Bitcoin increases by the day. Notably, Bitcoin can also be transferred from one person to the next anonymously.

Owners keep Bitcoins in a digital wallet. They can spend them on online, or they can trade their Bitcoins on exchanges. All Bitcoin transactions are recorded in a "blockchain," an online ledger that verifies each transaction's validity. Some collectors are holding Bitcoin, hoping the value of this cryptocurrency increases. The market is volatile. As of the writing of this article, a single Bitcoin is worth more than \$2,000 (up from a 2016 high of \$807). Although the price fluctuates, Bitcoin is designed to be insulated from inflation as the supply of Bitcoin is limited to 21 million.

The ability to transfer Bitcoins anonymously has led to it being the currency of choice for cybercriminals and for ransomware hackers. Cybercriminals need not worry about the payment being traced back to them. Payments between citizens of different countries is simplified because Bitcoins are not tied to any country's currency. Currently, Bitcoins are also effectively unregulated, meaning we are in the Wild West phase of Bitcoin's existence.

Ransomware or other invasive malware cannot spread to other parts of a network if there is no communication between them. Instruct your IT department or vendor to employ network segmentation.

Keep Computer Software Up to Date

WannaCry attacked a vulnerability in Microsoft's Windows operating systems. Microsoft distributed a patch aimed at closing this vulnerability in March. The worm did not affect users who installed the patch. Microsoft has been criticized for its initial response to users of older Windows versions. Although it eventually distributed free patches to these users (Microsoft normally charges for the support of older versions of its software), that move came too late for some to protect themselves against WannaCry. Updating from older versions of software and timely applying patches (or setting up automatic patching) will help protect against similar attacks.

Test Your Systems

Cities can check the status of their systems and try to find (and remedy) vulnerabilities before hackers exploit them. Commercial vendors offer "penetration testing," where the vendor tries to infiltrate a computer network just as a hacker would. Hackers often begin their efforts by social engineering, calling users at an organization and trying to get information from them that can be used to gain access to a network. Security vendors can also try social engineering techniques to pinpoint users who may give up such information.

Kentucky offers assistance to cities and local government organizations, including free penetration testing, said Jason Childers, director of the Kentucky Intelligence Fusion Center (KIFC). The KIFC is a collaborative effort of the Office of Homeland Security, Kentucky State Police, and other state and federal agencies. Through a partnership with federal agencies, the Kentucky Office of Homeland Security can assist cities in performing a "cyber resilience review" of their computer systems.

Childers also noted that the Office of Homeland Security is part of the recently formed Kentucky Cyber Threat Working Group, which meets to discuss current threats and means of dealing with them. The working group meets at 1:00 p.m. on the second Monday of every month. Any city interested in sending a representative to the meeting can contact Childers at 502.564.2081 or at jason.childers@ky.gov.

Segment Networks

Not all parts of your network need to be in communication with each other at all times, Childers said. Ransomware or other invasive malware cannot spread to other parts of a network if there is no communication between them. Instruct your IT department or vendor to employ network segmentation.

Back Up Data

The ability of a ransomware victim to avoid paying ransom depends on how well the victim's computer systems are backed up. Through its

partnership with KLC, Sophicity offers IT in a Box, which provides several services, including data backups and off-site data storage. Both can be critical in restoring computer systems without paying ransom. On-site backups will help a city recreate its data more quickly. Off-site backups may take longer but are part of a disaster response strategy, in the event a city's on-site backups are destroyed. "Other than someone's life being in jeopardy, data backup is our first priority," Mims said.

Share Risk by Insuring Against Cyberattacks

Traditional insurance products, such as a commercial general liability policy, or a public officials liability policy, generally do not cover cyber-related issues, such as ransomware attacks. But insurers now offer specific policies for cyber risks. KLC includes cyber coverage via an endorsement to its current policies. Other carriers offer cybersecurity insurance via separate policies. Whether the victim of a ransomware attack chooses to pay the ransom or to restore data, costs are associated with either choice. The right cyber insurance policy can pay or defray those costs and offer other resources for getting the insured back to full efficiency.

The difference between a natural disaster and a ransomware attack is that the latter is more predictable. "To think you're safe, that's false security," Mims said. "Ransomware is getting bigger because it's a huge moneymaker for bad guys."

If you are a victim of ransomware or any other kind of computer breach, Sunseri recommends immediately contacting the Kentucky Office of Homeland Security. "We have a system of resources through the state and federal agencies that can help." **KYC**

About the Authors



Barry Miller



Curtis Graham

Barry Miller and Curtis Graham are attorneys with Mazanec, Raskin & Ryder, L.P.A., Lexington, which supports KLC through its awards program sponsorship.

Miller's practice focuses on insurance coverage opinions and litigation, including coverage issues related to

municipal liability, bad faith and extra-contractual damages, and data management and cyber security law. He has considerable experience handling technology issues involving data breach defense and electronic discovery as well. He regularly provides instruction and counsel to a variety of groups, including attorneys and business owners, regarding preservation of digital evidence and insurance aspects of cyberliability. In 2017, he earned his accreditation as a Certified Information Privacy Professional/United States (CIPP/US), credentialed through the International Association of Privacy Professionals (IAPP). Contact: bmiller@mrllaw.com or 859.899.8513.

Graham focuses his practice on civil rights and governmental liability issues, including the representation of police officers, municipalities, correctional institutions and city officials. In addition to his representation of governments and government officials, Graham is experienced in all aspects of insurance litigation, ranging from coverage and bad faith disputes to insurance defense litigation. He has also handled matters of commercial law, subrogation, collections, data security and cybersecurity law. Contact: cgraham@mrllaw.com or 859.899.8516.

WE HELP GOVERNMENTS RUN MORE EFFICIENTLY

At Harshaw Trane, we specialize in innovative solutions, bringing critical cost savings and new revenue to local government buildings and systems through energy and operational efficiency and sustainability.

- Wastewater & water utilities
- Gas & electric utilities
- Building & street lighting
- Utility meter accuracy
- Heating, ventilating & air conditioning
- Controls & maintenance services

We invite you to talk with our team and learn how Harshaw Trane can help you energize your bottom line and empower your community.

www.harshawtrane.com

Visit us at klc.org.

EMPLOYER BENEFIT SOLUTIONS FOR THE PUBLIC SECTOR

Public sector professionals deserve a specialist.

For less worry, less work, and more expertise, consider American Fidelity for a different opinion.

Help is here.

- Strategic Voluntary Benefits
- Simplifying Technologies
- Employee Benefits, Education and Enrollment

Jared Levy
Government Markets Manager
800-654-8489, ext. 2432
americanfidelity.com

AMERICAN FIDELITY
a different opinion

American Fidelity Assurance Company