

**NEW JERSEY COUNTIES EXCESS JOINT INSURANCE FUND**

9 Campus Drive, Suite 216

Parsippany, NJ 07054

Telephone (201) 881-7632

**BULLETIN NJCE 18-07**

**Date: February 13, 2018**

**To: Fund Commissioners of NJCE**

**From: NJCE Underwriting Manager, Conner Strong & Buckelew**

**Re: Member Resources**

---

This will serve as a listing of resources from the NJCE's insurance partners and other sources available to members of the NJCE.

If you have any questions concerning this bulletin, please contact your Risk Management Consultant, Executive Director or the Underwriting Manager.

**This bulletin is for information purposes only. It is not intended to be all-inclusive but merely an overview. It does not alter, amend or change your coverage. Please refer to specific policies for limits, terms, conditions and exclusions.**

cc: Risk Management Consultants  
Professionals  
Executive Directors

## EMPLOYMENT PRACTICES LIABILITY

### **Chubb EPL Assist**

EPL Assist is a service available via Chubb for members with a Chubb Public Officials/EPL policy. EPL Assist is a cutting edge risk management program providing policyholders with access to a wide variety of legal content, forms and analysis, combined with the ability to interact directly with Littler lawyers dedicated to assisting Chubb insureds.

- No cost, online and live hotline access to legal experts at Littler
- A catalog of free online employment law resources
- Complimentary registration to Littler's breakfast briefing series webinar/podcast
- Discounted rates for various Littler events
- Employment law updates, newsletters and related publications
- Free, live training webinars on a myriad of topics

Visit [www.EPLAssist.com](http://www.EPLAssist.com), select "Request an Account" to register, and utilize your policy number for registration. After registration, you can either call or email the free hotline: 1-888-244-3844. Contacting this hotline does not constitute reporting of a claim. Please report all matters per your claim reporting guidelines.

A list of courses offered by Littler can be found attached to this bulletin.

# CYBER

## (Privacy & Network Security)

### Chubb Cyber Services

Chubb offers an array of free and for-cost cyber resources, as follows. Please review the attached Chubb Cyber Services – Loss Mitigation flyer and the Chubb Cyber Services – Signature Assessments flyer for more details.

- Password Defense – Chubb offers policyholders a password manager application for your desktop and mobile devices to make it easier for employees to create and use stronger passwords.
- Online Cyber Education – Access to two online cyber education courses (Security Awareness Basics and Security Awareness for Information Technology). Managers can download reports from the system to identify employee completion.
- Signature Assessments – Chubb offers consultative engagements at a flat rate, performed by industry-leading cyber service providers, including validating cyber incident response plans, identifying sensitive information, simulating a phishing attack, scanning for network vulnerabilities and monitoring cyber security scores.

Please contact the NJCE Underwriting Manager to engage the Signature Assessment resources. Chubb will do a matched reimbursement of the cost of a qualified service up to a maximum of \$3,000 per policy period. Reimbursements must be authorized by Chubb and will be made for only those services rendered 90 days prior to the policy expiration or renewal date.

Access Chubb's eRisk Hub powered by NetDiligence by sending an email request to [eriskhub@acegroup.com](mailto:eriskhub@acegroup.com) including the below information. After receiving your access code, go to [www.eriskhub.com/ace.php](http://www.eriskhub.com/ace.php) and complete the registration form.

- Your name
- Your title
- Your phone number
- Named Insured on your policy
- Your policy number

Also attached is a copy of Chubb's Cyber Incident Response Team list. **For urgent crisis management or legal advice, contact 1-800-817-2665 or [cyberalert@chubb.com](mailto:cyberalert@chubb.com).** Contacting this response coach hotline does not constitute reporting of a claim. Please report all matters per your claim reporting guidelines.

### Other Cyber Resources

- Data Privacy Day (provided by the National Cyber Security Alliance): <https://staysafeonline.org/>
- New Jersey Cybersecurity & Communications Integration Cell (NJCCIC): <https://www.cyber.nj.gov/>
- Government Technology (GovTech): <http://www.govtech.com/>
- Stu Sjouerman Blog: <https://about.me/StuSjouerman>
- Netwrix's Government IT Risks report for 2017 is attached
- CSB Email Dos & Don'ts Infographic is attached (share with all employees)

A Guide to Lawfully Hiring the Best Candidates

---

A Supervisor's Guide to Understanding, Preventing and Correcting Abusive Conduct, Sexual and Unlawful Harassment, Discrimination and Retaliation

---

Conducting Lawful Investigations: A Comprehensive Workshop for Internal Investigators

---

Dynamic Conflict Resolution Skills for Workplace Problems

---

I-9 Compliance and ICE Audits

---

Maintaining an Equal Opportunity Workplace

---

Maintaining and Managing a Respect-Based Workplace

---

Managing Abusive Conduct in the Workplace (The California Anti-Bullying Law)

---

Managing Employee Medical and Family Concerns — ADA/FMLA

---

Managing, Motivating, and Improving Performance

---

Managing Positive Employee Relations in a Union-Free Workplace

---

Managing Wage and Hour Essentials

---

Managing Within the Law: Merging Employment Law Fundamentals with Management Essentials

---

Proper Practices and Potential Pitfalls for Navigating Social Media in the Workplace

---

Safe, Respectful and Lawful Approaches to Termination Decisions

---

Safe Workplace — Violence, Bullying and Respect: Manager & Employee Programs

---

Supervising in America: For the International Manager

---

What Every Employee Should Know About a Workplace Free of Harassment & Retaliation

---

\* Additional courses based on employment law fundamentals and leadership essentials may be customized to meet the client needs. Please e-mail [contact@littler.com](mailto:contact@littler.com) to discuss how we can use our Global Littler resources to meet your training and compliance needs.

# Course List (cont.)

Littler Learning Group (LLG) was created to merge best practices with employment law fundamentals. We work closely with clients to ensure that each learning experience matches the organization's objectives, core values, culture and work environment by providing a range of services:

- Live Employment Law and Management Training by Littler Attorneys: In-Person/Webinar
- Train-the-Trainer Services & Custom Training Projects
- Consent Decree Fulfillment & Court-Ordered Programs
- Coaching and Counseling Sessions for Executives and Managers
- Diversity and Inclusion Services
- Wide-Ranging Facilitation Services: Focus Groups, Team Building, Leadership Development
- In-house Video Production Services: Standard & Customized Training Content
- Blended Solutions: Combining Live & E-Learning
- Multilingual Programs Presented Internationally
- Custom E-Learning and self-study programs upon request.

Please contact LLG at [contact@littler.com](mailto:contact@littler.com) for additional information



**Kevin O'Neill**  
Sr. Director-LLG, Principal  
KONeill@littler.com • 415.288.6322



**Marissa Dragoo**  
LLG, Special Counsel  
MDragoo@littler.com • 916.830.7245



**Cindy-Ann Thomas**  
Principal  
CATHomas@littler.com • 704.972.7026



**Karen Sundermier**  
Knowledge Management Counsel  
KSundermier@littler.com • 617.378.6093



**Michael Moorman**  
Training Specialist  
MMoorman@littler.com • 816.772.0996



**Tess Richardson**  
Marketing Coordinator  
TRichardson@littler.com • 816.772.0833

## ABOUT LITTLER

Littler is the largest global employment and labor law practice, with more than 1,200 attorneys in over 75 offices worldwide. Littler represents management in all aspects of employment and labor law and serves as a single-source solution provider to the global employer community. Consistently recognized in the industry as a leading and innovative law practice, Littler has been litigating, mediating and negotiating some of the most influential employment law cases and labor contracts on record for 75 years. Littler Global is the collective trade name for an international legal practice, the practicing member entities of which are separate and distinct professional firms. For more information visit [littler.com](http://littler.com).

**Littler Learning Group**

Compliance Training Solutions Worldwide

[contact@littler.com](mailto:contact@littler.com) | [littler.com/service-solutions/littler-learning-group](http://littler.com/service-solutions/littler-learning-group)

2.2017

# Cyber Services

## Loss Mitigation for Cyber Policyholders

CHUBB®



At Chubb, we believe that being prepared for a cyber incident can go a long way in limiting losses when one occurs. To complement our superior insurance protection, we offer enhanced benefits and services through various third party service providers to deliver extra assurance and specialized attention for our cyber policyholders.

### **Password Defense**

---

Chubb offers policyholders a password manager application for your desktop and mobile devices to help improve cyber security by making it easier for employees to create and use stronger passwords. Motivate individuals to keep healthier password habits by generating strong passwords for websites, storing them in a secure vault and synchronizing them across multiple devices. This system encourages employees not to write down or reuse passwords.

### **Password Defense: FAQs**

*How does the application strengthen passwords?*

The application's Security Dashboard provides metrics of overall password health, helping individuals easily identify and replace weak or reused passwords.

*How are passwords added to the password manager?*

Passwords are entered manually through the application on any browser. Individuals can also import passwords that are stored in a browser or other password manager applications.

*How does the application secure passwords?*

The patented architecture is built to ensure only the account holder can access his/her passwords.

*How much does password defense cost?*

The offer is complimentary for Chubb's cyber policyholders.

## Online Cyber Education

---

Chubb's cyber policyholders have access to two online cyber education courses that can be quickly and easily deployed to educate employees: Security Awareness Basics and Security Awareness for Information Technology. The online training teaches the basics of:

- Identifying potential threats
- Protecting sensitive data
- Escalating issues to the right people when necessary

Managers are able to download reports from the system to identify who has completed the courses.

### Online Cyber Education: FAQs

*Who can access the courses?*

Both courses can be made available to all employees.

*Can employees print certificates when they complete a course?*

Yes, certificates can be printed to show that an employee has completed the course.

*How long does it take to complete each course?*

Each course has been designed to take approximately 20 to 30 minutes.

*Can additional courses be added to the training portal?*

Yes, additional courses are available for purchase.

*How much does online cyber education cost?*

The offer is complimentary for Chubb's cyber policyholders.

## Signature Assessments

---

Packaged assessments help Chubb's cyber policyholders quickly gauge and understand key areas of risk. These cost-effective, consultative engagements are offered at a flat rate and are performed by a select group of industry-leading service providers. Signature assessments are available for the following:

- Validating a cyber incident response plan
- Identifying sensitive information
- Simulating a phishing attack
- Scanning for network vulnerabilities
- Monitoring cyber security scores

### Signature Assessments: FAQs

*Are the assessments completed remotely or onsite?*

The assessments are designed to be completed remotely. Some providers can complete assessments onsite if necessary.

*Does hardware or software have to be installed for the assessments?*

No. Assessments can be performed without installations or downloads.

*Does Chubb see the results of the signature assessments?*

No, Chubb does not receive a copy of the results.

*Can policyholders expand the scope of services?*

Yes. Policyholders can work directly with each provider to expand the package as needed.

*How much does each signature assessment cost?*

Chubb's cyber policyholders are able to access assessments at a flat rate of \$3,000 each.

## Contact Us

---

To learn more about Chubb's cyber services, email us at [chubb@cyber.com](mailto:chubb@cyber.com) or visit [www.chubb.com/us/cyber](http://www.chubb.com/us/cyber).

**Chubb. Insured.<sup>SM</sup>**

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit [www.chubb.com](http://www.chubb.com). Chubb's cyber services cannot be construed to replace any provisions of your policy. You should read your policy, including all attachments, for complete information on the coverage parts provided. Chubb has no obligation to provide any of the cyber services. The policyholder is under no obligation to contract for services with any of the service providers. The selection of a particular pre-approved Loss Mitigation Services vendor is the independent choice of the policyholder. Neither Chubb nor its employees or agents make any warranties or assume any liability for the performance of the pre-approved vendor, including any goods or services received. Chubb does not endorse vendors or their respective services. Before a policyholder engages with vendors, the policyholder should conduct its own due diligence to ensure the company and its services meet its needs. Unless otherwise indicated or approved, payment for services provided by any vendor is the responsibility of the policyholder. Copyright©2016 617502

(Rev. 12/16)

# Cyber Services for Loss Mitigation

## Signature Assessments Overview



Welcome to Chubb's Cyber Services for Loss Mitigation! We offer these services because we believe that being ready to respond will help reduce the exposure to a loss when a cyber event occurs. As a Chubb cyber policyholder, you have access to a suite of **Loss Mitigation Services** to help mitigate potential cyber exposures *before* an event happens as well as several **Signature Assessments** which can help your organization quickly gauge and understand key areas of cyber risk. Loss Mitigation services are provided directly to your organization by a panel of Chubb pre-approved vendors at a pre-negotiated flat rate. For a complete list of services, please visit: [www.chubb.com/us/cyberservices](http://www.chubb.com/us/cyberservices).

### Response Readiness Assessment

|                      |  |
|----------------------|--|
| Delivered by Fidelis | <p>Evaluate your organization's response plan or get started creating one.</p> <p>Fidelis Cybersecurity will provide a personalized consultation to walk your organization through a streamlined process and assess your incident response plan based on industry standards. In cases where a response plan does not already exist, Fidelis will help your organization through a process to jump start the development of one.</p> <p>Fidelis will first request that your organization execute a mutual non-disclosure agreement to establish a confidential relationship with your organization. Fidelis will then provide its multipart assessment for your organization to complete. The assessment will include requests for any existing incident response plan documentation that Fidelis can include in the overall review. Fidelis will then conduct a review of the materials, focusing on the internal and external response capabilities of your organization. The final report will include findings and suggested action items for your organization to remediate. The scope includes missing documents, technical and software recommendations and regulatory benchmarks.</p> <p>More information on Fidelis can be found at <a href="http://www.fideliscybersecurity.com">www.fideliscybersecurity.com</a>.</p> |
|----------------------|--|



| Security Performance Benchmarking |   |
|-----------------------------------|---|
| Delivered by BitSight             | <p>Monitor the security of your organization and third party vendors through external data gathered from the public Internet.</p> <p>Cyber policyholders receive a personalized login to the BitSight portal for 12 months, allowing you to continuous monitoring of their organization and up to three vendors of their choice.</p> <p>BitSight’s online platform continuously analyzes, rates and monitors the security posture of organizations, all from the outside. Ratings are generated on a daily basis, giving continuous visibility into the performance of your security program. With the ability to determine the security details used to generate your organization’s rating, pertinent security issues can be mitigated and tracked over time.</p> <p>More information on BitSight can be found at <a href="http://www.bitsighttech.com">www.bitsighttech.com</a>.</p>   |
| Network Vulnerability Testing     |   |
| Delivered by NetDiligence         | <p>Assess vulnerabilities on your external network - a common method threat actors use to gain access to organizations’ networks.</p> <p>NetDiligence will conduct an automated vulnerability scan of up to eight external network addresses that represent some of your organization’s external systems, such as firewalls, web applications and mail servers. Once the scan is completed, an Interpretive Summary Report is generated to bring together the key points and risk factors that should be prioritized for remediation. In addition to the summary report, the “raw” results are also provided to help your IT Staff validate and remediate the findings. Additional internal scanning options are available but require the assistance of on-site IT/networking personnel who can perform installation and placement of a “virtual scanner software” on the internal network.</p> <p>More information on NetDiligence can be found at <a href="http://www.netdiligence.com">www.netdiligence.com</a>.</p>  |
| Phishing Simulation               |   |
| Delivered by PhishMe              | <p>Test a sample of your employees to see how well they respond to a simulated phishing attack.</p> <p>Electronic mail continues to be used by threat actors as a primary delivery mechanism to entice employees to click on malicious links or attachments. For the unaware employee, taking action on these malicious emails can lead to malware infection, theft of usernames/passwords or cyber extortion via ransomware.</p> <p>For this effort, PhishMe will work with your organization to run two phishing simulations over the course of four months: (1) a <i>Click Only</i> scenario where an email urges the recipient to click on an embedded link; and (2) a <i>Data Entry</i> scenario where an email containing a link to a customized landing page entices the user to enter their valid credentials (e.g., user ID, passwords), allowing the attacker to gain access to an organization’s network environment. Individuals who fall victim to the simulation are directed to complete online training material on phishing and its effects on company security. At the conclusion of each simulation, PhishMe will provide your organization with a report containing extensive analytics, including an executive summary, simulation findings and a response analysis that details the overall susceptibility rate, reporting rate, and the repeat offense rate. No user-sensitive data is stored during simulations.</p> <p>More information on PhishMe can be found at <a href="http://www.phishme.com">www.phishme.com</a>.</p> |

**Chubb. Insured.<sup>SM</sup>**

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit [www.chubb.com](http://www.chubb.com). Chubb’s cyber services cannot be construed to replace any provisions of your policy. You should read your policy, including all attachments, for complete information on the coverage provided. Chubb has no obligation to provide any cyber services for loss mitigation. The policyholder is under no obligation to contract for services with any of the Chubb pre-approved loss mitigation service providers. The selection of a particular loss mitigation service provider is the independent choice of the policyholder. Chubb is not a party to any agreement entered into between any loss mitigation service provider and the policyholder. It is understood that loss mitigation service providers are independent contractors, and not agents of Chubb. Chubb assumes no liability arising out of any services rendered by a loss mitigation service provider. Chubb shall not be entitled to any rights, or subject to any obligations or liabilities, set forth in any agreement entered into between any loss mitigation service provider and the policyholder. Any rights and obligations with respect to such agreement, including but not limited to billings, fees and services rendered, are solely for the benefit of, and borne solely by, such loss mitigation service provider and the policyholder, and not Chubb. Neither Chubb nor its employees or agents make any warranties or assume any liability for the performance of any loss mitigation service provider, including any goods or services received. Chubb does not endorse the loss mitigation service providers or their respective services. Before a policyholder engages with any loss mitigation service provider, the policyholder should conduct its own due diligence to ensure the company and its services meet the policyholder’s needs.

Form 14-01-1244 (Rev. 9/17)

# Cyber Services

## Cyber Incident Response Team

CHUBB®



Chubb's Cyber Incident Response Team is comprised of experienced service providers including Computer Forensics, Public Relations, Notification-Identity Services, Call Center Services, Cyber Extortion-Ransom, Business Interruption, Legal-Regulatory Communications. Chubb's Cyber Incident Response Team shall be construed as part of your policy, but no coverage is provided by this Cyber Incident Response Team nor can it be construed to replace any provisions of your policy. You should read your policy, including all attachments, for complete information on the coverage parts you are provided.

Chubb has no obligation to provide any of the legal, computer forensics, public relations, notification-identity services, call center services, cyber extortion-ransom, business interruption, legal-regulatory communications by the Cyber Incident Response Team. The policyholder is under no obligation to contract for services with Cyber Incident Response Team service providers, except as amended by the Cyber Incident Response Team Endorsement.

### **Response Team Hotline**

(800) 817-2665

## Response Team Coaches

| Provider               | Primary Contact       | Phone          | Email                                 |
|------------------------|-----------------------|----------------|---------------------------------------|
| BakerHostetler         | Theodore J. Kobus III | (212) 271-1504 | tkobus@bakerlaw.com                   |
| Borden Ladner Gervais* | Ira Nishisato         | (844) 617-1887 | inishisato@blg.com                    |
| Fasken Martineau*      | Alex Cameron          | (844) 200-7505 | acameron@fasken.com                   |
| Mullen Coughlin        | John Mullen           | (267) 930-4792 | jmullen@mullen.legal                  |
| Norton Rose Fulbright  | Dave Navetta          | (303) 801-2732 | david.navetta@nortonrosefulbright.com |

\* Canada

## Response Team Specialists

| Provider                 | Primary Contact | Phone          | Email                            | Team Specialty                   |
|--------------------------|-----------------|----------------|----------------------------------|----------------------------------|
| Allclear ID              | Allen Burzen    | (512) 897-8208 | allen.burzen@allclearid.com      | Individual Notification Services |
| Alvarez & Marsal         | Art Ehuan       | (571) 331-7763 | aehuan@alvarezandmarsal.com      | Computer Forensics               |
| CGI*                     | Gary Miller     | 613- 740-5742  | gary.w.miller@cgi.com            | Computer Forensics               |
| Charles River Associates | Bill Hardin     | (312) 619-3309 | bhardin@crai.com                 | Computer Forensics               |
| CrowdStrike              | Charlie Groves  | (303) 887-0506 | charlie.groves@crowdstrike.com   | Computer Forensics               |
| Cyintelligence*          | Daniel Tobok    | (647) 846-0889 | dtobok@cyintelligence.ca         | Computer Forensics               |
| Dashlane                 | David Sawin     | (919) 928-2184 | david.sawin@dashlane.com         | Individual Notification Services |
| Davis Wright Tremaine    | Amy Mushahwar   | (202) 973.4263 | amymushahwar@dwt.com             | Legal & Regulatory Comms.        |
| Edelman Canada           | Greg Vanier     | 416-849-3337   | greg.vanier@edelman.com          | Public Relations                 |
| Equifax*                 | Timothy Walsh   | 416-505-7386   | timothy.walsh@equifax.com        | Individual Notification Services |
| Experian                 | Ozzie Fonseca   | (949) 567-3851 | ozzie.fonseca@experian.com       | Individual Notification Services |
| Fidelis Cybersecurity    | Rex Brunelli    | (210) 365-6884 | rex.brunelli@fidelissecurity.com | Computer Forensics               |
| FireEye/Mandiant         | Karen Kukoda    | (916) 458-2030 | karen.kukoda@fireeye.com         | Computer Forensics               |
| Kivu Consulting, Inc.    | Shawn Melito    | (814) 207-4007 | smelito@kivuconsulting.com       | Computer Forensics               |

Chubb. Insured.<sup>SM</sup>

Chubb shall not be a party to any agreement entered into between any Cyber Incident Response Team service provider and the policyholder. It is understood that Cyber Incident Response Team service providers are independent contractors, and are not agents of Chubb. The policyholder agrees that Chubb assumes no liability arising out of any services rendered by a Cyber Incident Response Team service provider. Chubb shall not be entitled to any rights or subject to any obligations or liabilities set forth in any agreement entered into between any Cyber Incident Response Team service provider and the policyholder. Any rights and obligations with respect to such agreement, including but limited to billings, fees and services rendered, are solely for the benefit of, and borne solely by such Cyber Incident Response Team service provider and the policyholder, and not Chubb. (Rev. 10/16)

|                     |                    |                |                               |                                  |
|---------------------|--------------------|----------------|-------------------------------|----------------------------------|
| KPMG*               | John Perea         | 416.777.8736   | johnperea@kpmg.ca             | Computer Forensics               |
| Kroll               | Jennifer Rothstein | (212) 833-3456 | jrothstein@kroll.com          | Computer Forensics               |
| LEVICK              | Megan Gabriel      | (202) 973-5308 | mgabriel@levick.com           | Public Relations                 |
| Marshall Dennehey   | David J. Shannon   | (215) 575-2615 | djshannon@mdwecg.com          | Legal & Regulatory Comms.        |
| Navigant Consulting | Darin Bielby       | (215) 832-4485 | dbielby@navigant.com          | Computer Forensics               |
| NPC                 | Larissa Crum       | (866) 377-8210 | larissa.crum@immersionltd.com | Call Center Services             |
| RSM                 | Daimon Geopfert    | (248) 802-4908 | daimon.geopfert@rsmus.com     | Computer Forensics               |
| Stroz Friedberg     | Bryan Rose         | (212) 981-6549 | brose@strozfriedberg.com      | Computer Forensics               |
| The Ackerman Group  | Wes Odom           | (305) 298-2117 | wodom@ackermangroup.com       | Cyber Extortion and Ransom       |
| TransUnion          | Gillian Johnson    | (312) 985-3629 | gjohnso@transunion.com        | Individual Notification Services |
| Verizon             | Christopher Novak  | (877) 330-0465 | chris.novak@verizon.com       | Computer Forensics               |

\* Canada

**Chubb. Insured.<sup>SM</sup>**

Chubb shall not be a party to any agreement entered into between any Cyber Incident Response Team service provider and the policyholder. It is understood that Cyber Incident Response Team service providers are independent contractors, and are not agents of Chubb. The policyholder agrees that Chubb assumes no liability arising out of any services rendered by a Cyber Incident Response Team service provider. Chubb shall not be entitled to any rights or subject to any obligations or liabilities set forth in any agreement entered into between any Cyber Incident Response Team service provider and the policyholder. Any rights and obligations with respect to such agreement, including but limited to billings, fees and services rendered, are solely for the benefit of, and borne solely by such Cyber Incident Response Team service provider and the policyholder, and not Chubb. (Rev. 10/16)



# EMAIL DOs & DON'Ts



## EMAIL ADDRESSES

- Do you recognize the sender and the CCs?
- Is the sender's email spelled correctly? (i.e. "YourMayor" vs. "YourMay0r")

## DATE & TIME

- Was the email sent on a typical day and at a typical time?

## EMAIL CONTENT

- Are the format and grammar in the email typical for the sender?
- Does the content seem atypical?
- Did the sender seem overly urgent?
- Does the email ask for person info/login info?

From: YourMayor@yourtown.com  
 To: You@yourtown.com  
 Cc: Who@where.com, Who2@Site.com, Who3@Web.com  
 Date: Sunday, October 3, 2105 at 3:20 a.m.  
 Subject: Wire for Project

Message | Instructions.docx (4 KB)

Hi,  
 Im traveling and lost my phone. We need to wire money for a large project to the below link ASAP so the project isnt delayed.  
 Could you wire \$15,000 today?

<http://www.chase.com>

Thanks so much.  
 Mayor

## SUBJECT

- Is the subject a typical style for the sender?
- Does the subject match the email content?

## ATTACHMENT

- Is an attachment needed for the email content?
- Were you expecting the attachment?
- Is it a ".txt" file?

## LINKS

- Does the link look appropriate?
- Does the web address match the hyperlink shown (scroll over the hyperlink)?

## DON'T GET PHISHED!

... but if you do, remember to

Contact Your Conner Strong & Buckelew Claims Representative for reporting the claim and engaging breach counsel and forensics firms as necessary.

CONNER  
 STRONG &  
 BUCKELEW

## CONTEXT

**88%** **88%** **75%**

Of organizations do not use any software for information security governance or risk management

Of IT operations teams are at least partially responsible for security

Of organizations do not have a separate information security function

## MAIN SECURITY FOCUS



Mobile devices

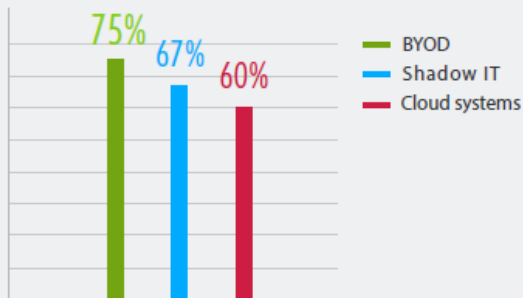


Endpoint



On-prem systems

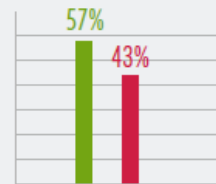
## MOST NEGLECTED AREAS



100%  
Employees

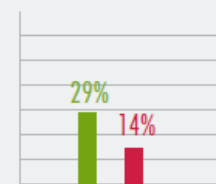
**33%** of organizations had compliance issues in 2016

## MAIN CAUSES OF SECURITY INCIDENTS IN 2016



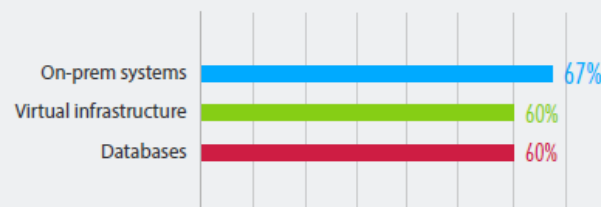
Human errors  
Insider misuse

## MAIN CAUSES OF SYSTEM DOWNTIME IN 2016



A system was down unacceptably long or outages happened too often  
Accidental or incorrect user activity

## WHERE VISIBILITY INTO USER ACTIVITY IS MOST NEEDED



ONLY **14%** of organizations are well prepared to beat cyber risks

## WHY?



57%

Lack of time



54%

Lack of budget



43%

Complexity of IT infrastructure



43%

Growth of data assets

## FOCUS OF FUTURE INVESTMENTS



43%

Intellectual property theft



29%

Data breach



14%

Fraud

## WHY ORGANIZATIONS NEED VISIBILITY



86% To detect and mitigate human factor (errors, misuse, etc.)

71% To investigate security incidents

71% To optimize IT processes and operations