Kroll | A Division of DUFF & PHELPS

Cyber Insurance Coverage: Securing the Right Policy for Your Risks

May 30, 2019

- Keith Novak, Associate Managing Director, Cyber Risk, Kroll
- Vinny Sakore, Chief Technology Officer, NetDiligence

Presenters

Keith Novak
Kroll

Contact:
keith.novak@kroll.com

Keith Novak has worked in the information technology field for more than 25 years, and is an accomplished manager and practitioner with extensive experience designing, implementing and securing systems and networks.

In his current role, Keith partners with clients at the strategic, operational and technical levels to proactively build information security programs and help reduce risk according to organizational needs while complying with regulatory requirements. He has special expertise in healthcare information technology and is highly proficient in the technical and regulatory requirements relating to Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI) compliance.

Vinny Sakore
NetDiligence

Contact:
vinny.sakore@netdiligence.com

Vinny Sakore joined NetDiligence® as Chief Technology Officer (CTO) in May 2017. Prior to NetDiligence, Mr. Sakore served as Verizon's HIPAA Security Officer and a member of Verizon's Cyber Security Strategy and Risk team.

Vinny is an active member of both the International Association of Privacy Professionals (IAPP) and the Healthcare Information Management and Systems Society (HIMSS). He serves on several non-profit boards, including the Central Pennsylvania HIMSS Chapter and Life Center Ministries International.

Vinny is a featured speaker nationally and internationally on the topics of Cyber Risk, Cloud Security, and HIPAA Security. He is a regular presenter at organizations such as the Information Security Forum (ISF), IAPP, HIMSS, and the Risk Information Management Society (RIMS).

Outline

- Cyber claims study
- Risk areas most often overlooked – and how to address
- How to conduct a risk assessment that underwriters will take seriously
- Evaluating existing coverage for potential gaps – and how to negotiate adjustments
- Benefits of cyber insurance in a time of crisis

BEC Scammers Steal US$1.75 Million From an Ohio Church

May 02, 2019

BEC threat actors are expanding from their traditional enterprise victims toward nonprofit and religious or involving a

Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.

Nation state attacks – the cyber cold war gets down to business

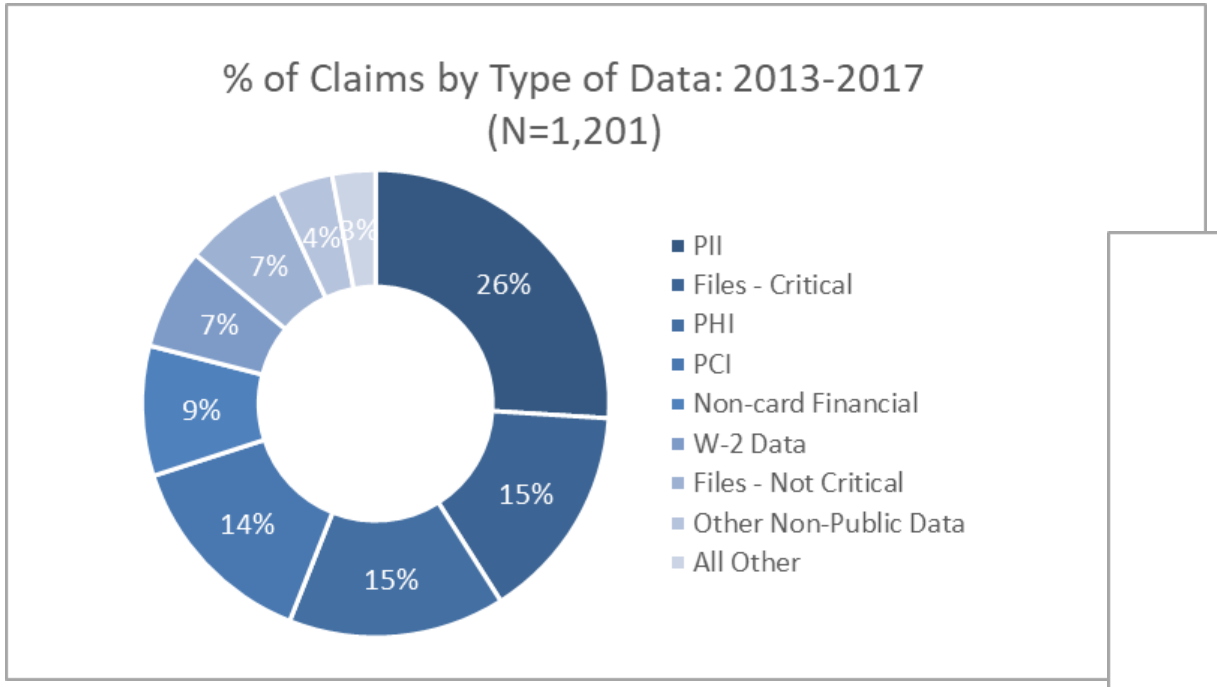
Cyber weaponry is moving to new frontiers: yours. Businesses are the next target on the nation state menu. Are you protected or vulnerable?

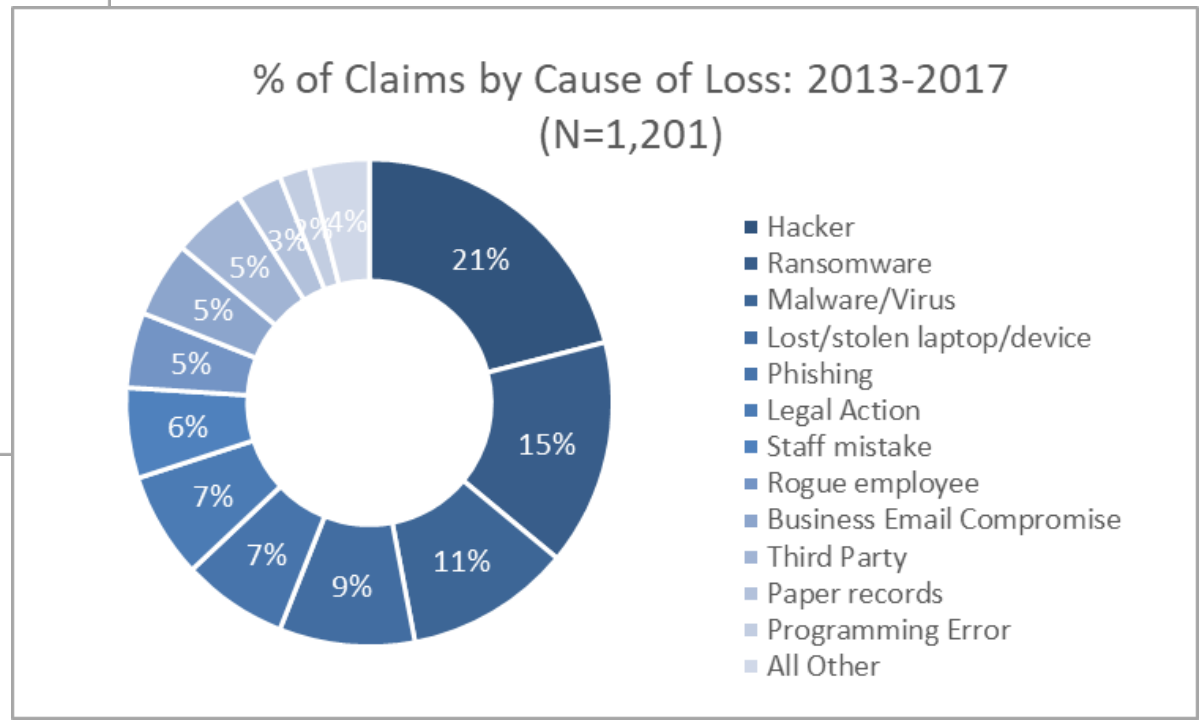
Cyber Insurance Not Valid in Case of Cyber War, Says Major Insurance Company

Baltimore ransomware nightmare could last weeks more, with big consequences

Houses can't be sold, bills can't be paid while city networks are shuttered.

NetDiligence® 2018 Cyber Claims Study



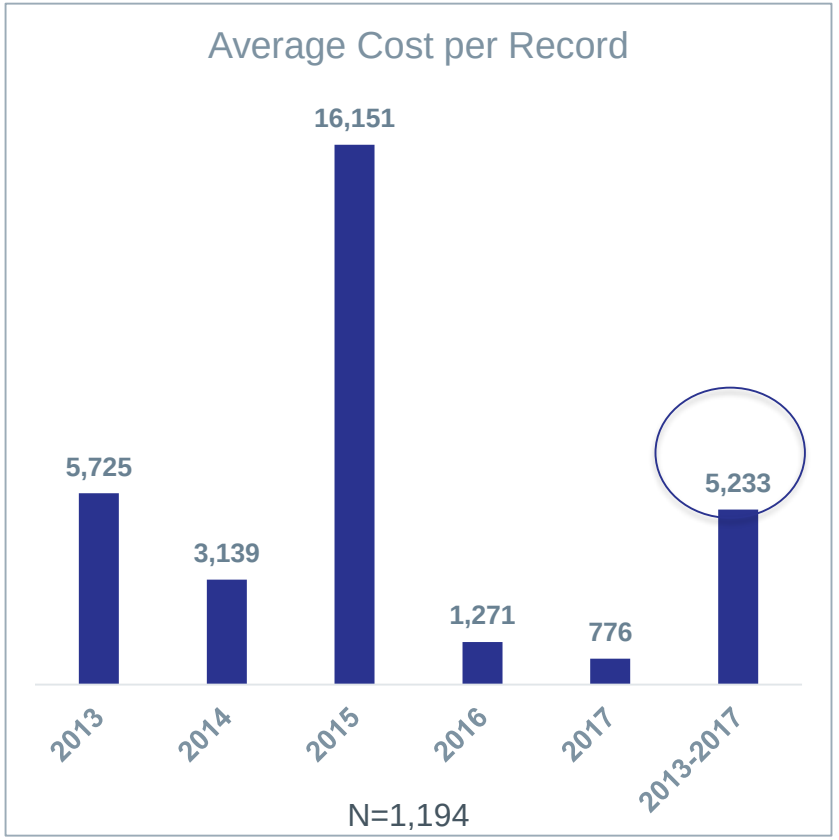


NetDiligence® 2018 Cyber Claims Study

- Claims Submitted 1,201

- Per-Breach Costs
  - 5-Year Average $603.9K
  - 2017 1-Year Average $603.7K
  - 2017 1-Year Average – Large Co. $24.6M
    (median $17.2M)

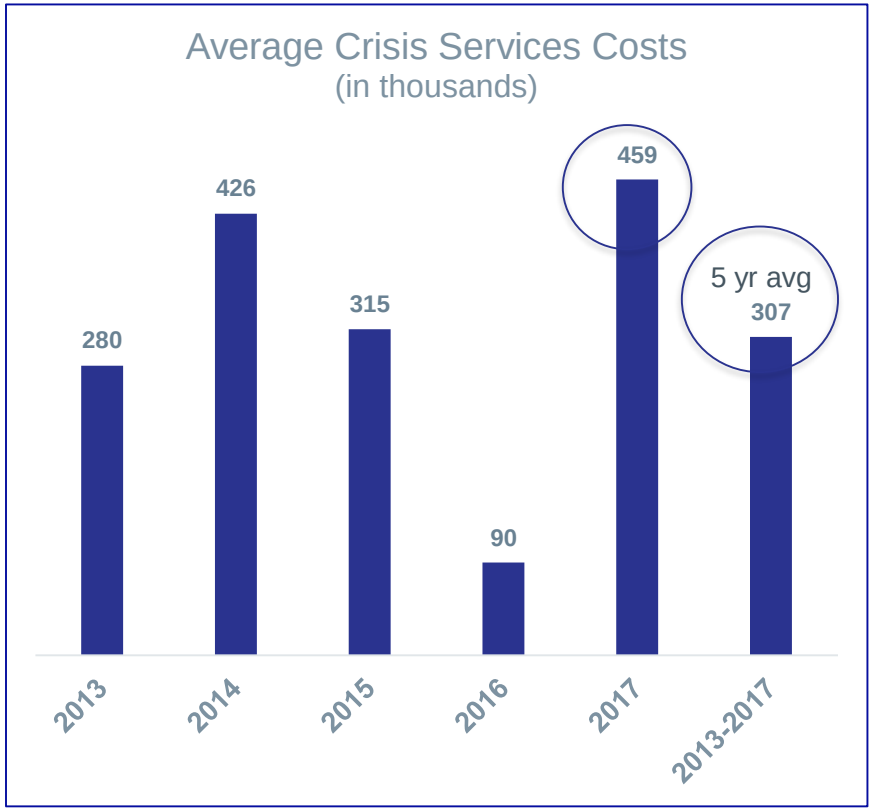
- Per-Record Costs
  - 5-Year Average $5.2K
    (median $43)
  - Cost Range $0.001-$1.6M



NetDiligence® 2018 Cyber Claims Study

- Crisis Services
  (forensics, legal counsel, notification, ID/credit monitoring, etc.)
  - 5-Year Average $307K
  - 2017 1-Year Average $459K

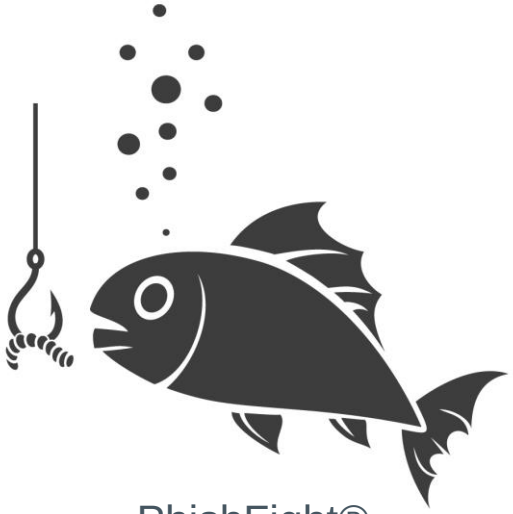
- Legal Costs – 5-Year Averages
  (defense & settlement)
  - Legal Defense $106K
  - Regulatory Defense $514K
  - Settlement $224K



NetDiligence® 2018 Cyber Claims Study

- Phishing/BEC/Social Engineering (N=164)
  - 5-Year Average Breach Cost $99K *(median $48K)*

- Ransomware (N=186)
  - 5-Year Average Ransom Demand $23K
  - 5-Year Average Breach Cost* $229K
    - » When ransom is paid by Insurer *(w/preferred vendor)* $92K
    - » When ransom is not paid at all $211K



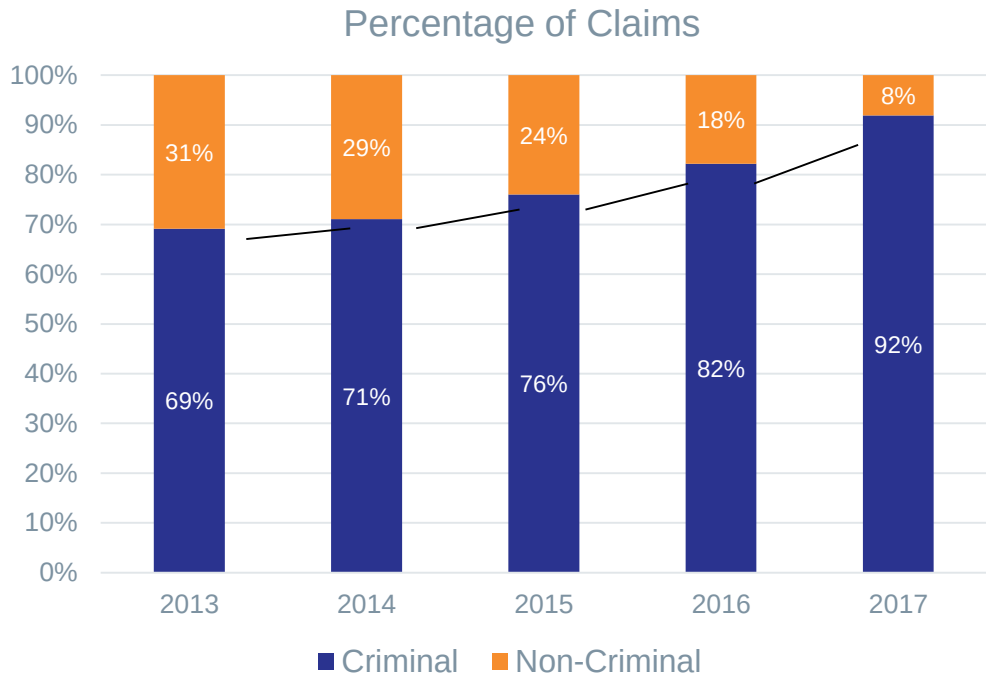
PhishFight®
See in eRiskHub®

* ***Some Example Cost-Driving Factors***
- Insured decides system affected (infected) not worth recovery, does little.
- Outside Forensics team used to restore from back up: preferred method and often least expensive
- Insureds own IT team restores from back-up (without experts)
- Insureds own IT team pays ransom and attempts to restore but decryption key fails, or doesn't pay ransom and backups fail.

A Note on Cybercrime

Insurance Industry Cybercrime Task Force (IICTF), sponsored by NetDiligence®

- Ransomware demands explode in 2018
  - Demands of $250K-$500K (nonexistent 6 months ago) now a weekly occurrence (Kivu)
  - Top ransomware payouts began to exceed $1M, dwarfing the previous max of $17K (Chubb)



- Top cybercrime-related causes
  - Ransomware – 31%
  - Phishing/BEC/Social Engineering – 24%
  - Hacking – 19%
  - Malware/Virus – 11%

Risk areas most often overlooked – and how to address

- **Cloud Adoption**
  - Multifactor Authentication
  - Security Assessments
  - Penetration Testing
- **Mobile Devices**
  - Encryption
- **Personal Devices (BYOD)**
  - Mobile Device Management
- **Insider Threats**
  - Data Loss Prevention
  - Security Analytics

How to conduct a risk assessment that underwriters will take seriously

- **What do underwriters look for?**
  - What types of information (with regard to customers and employees) does the Applicant collect, process and store?
  - Does your organization identify where sensitive information is collected, stored, and transported on your network?
  - Does your organization encrypt sensitive, confidential, or personally identifiable information (PII)?
  - Does your organization encrypt all portable computing devices, e.g. laptops, smartphones, tablets, etc.?
  - Has the applicant conducted a security assessment or audit in the last 12 months?

How to conduct a risk assessment that underwriters will take seriously

- **Conduct an enterprise wide risk assessment**
  - Inventory data
  - Assess regulatory requirements
  - Adopt a formal risk management framework
  - Perform a risk based assessment (NIST, CIS)
  - Build a Security Risk Register
  - Establish a vulnerability management program

Evaluating existing coverage for potential gaps – and how to negotiate adjustments

ASK:

- What are you most concerned about if you were to be a victim of a cyber incident? Losing PII? Business Interruption? Notifying Customers? Fine and Penalties? Reputational Damage?

EVALUATE:

- Now take a look at your coverage and see if you are covered and if you are, what limits apply to your concerns. Do you have full limit for PII? How long is the waiting period for Business Interruption before the coverage kicks in? **Is notification covered on your policy?**

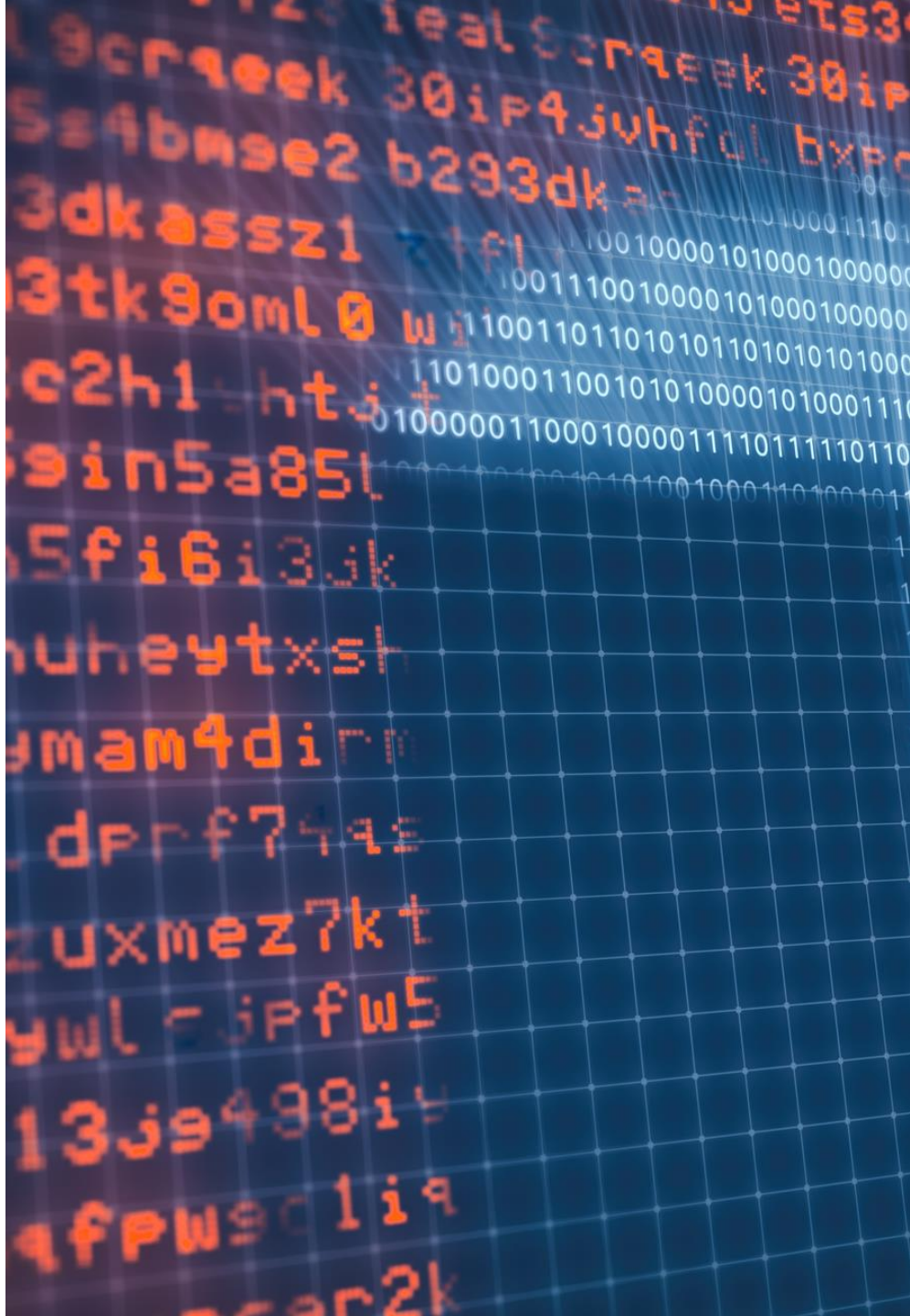
NEGOTIATE ADJUSTMENTS:

- Are there higher limits and/or coverages that don't apply to your business that you could remove completely or reduce coverage for and use the reduction in premium to increase a bigger area of concern?

- Are there proactive measures you can implement to reduce your risk and receive a reduction in premium?

Benefits of cyber insurance in a time of crisis

- **Pre-negotiated rates**
- **Single point of contact to start response efforts**
  - **Panel of experts**
    - Legal *(Breach Coach)*
    - Public Relations
    - Forensics / Incident Response
    - eDiscovery
    - Notification *(Letters, Call Centers, Credit Monitoring)*




Q
&
A

Kroll | A Division of DUFF & PHELPS

For more information about our global locations and services, please visit:
www.kroll.com

> keith.novak@kroll.com

> vinny.sakore@netdiligence.com

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. For more information, visit www.kroll.com.

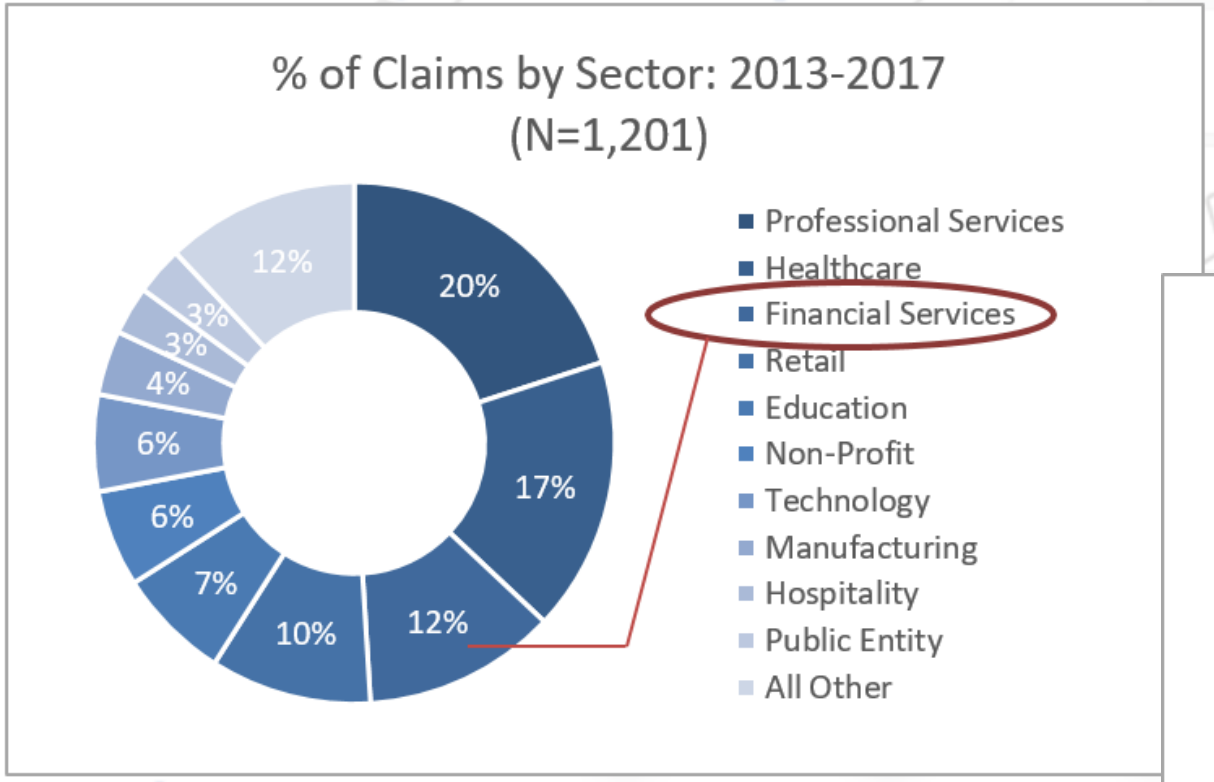
About Duff & Phelps

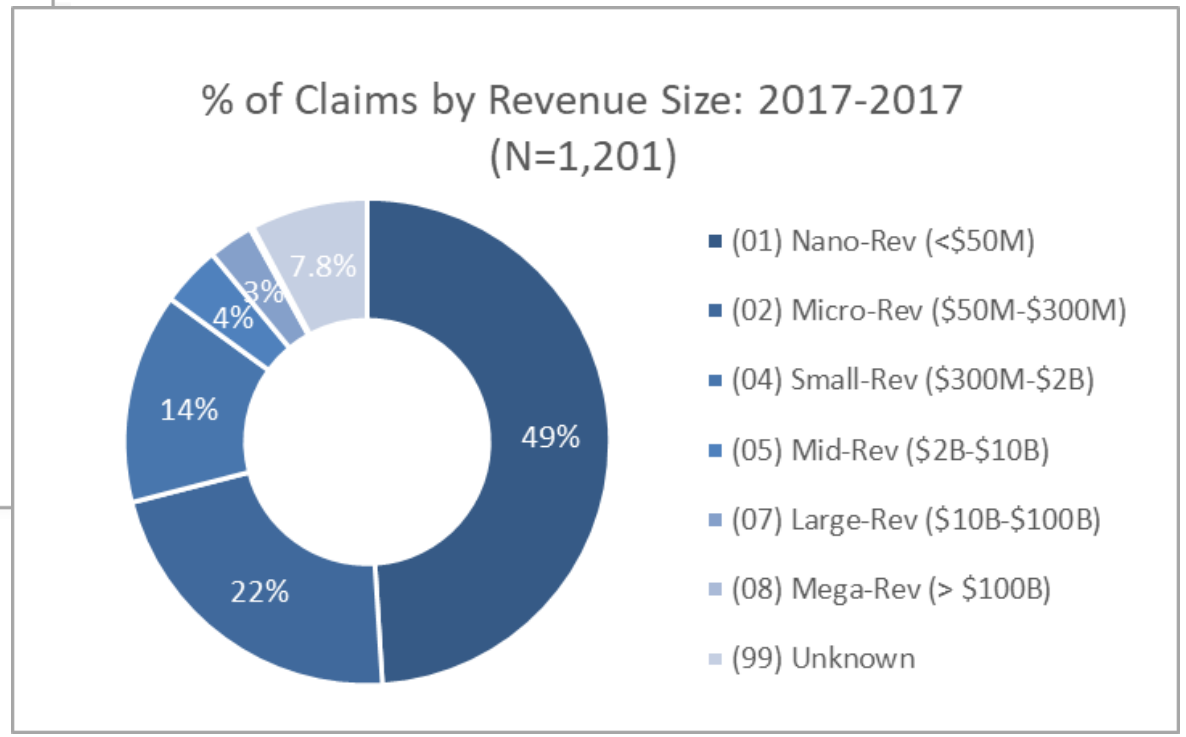
Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, investigations, disputes, cyber security, compliance and regulatory matters, and other governance-related issues. We work with clients across diverse sectors, mitigating risk to assets, operations and people. With Kroll, a division of Duff & Phelps since 2018, our firm has nearly 3,500 professionals in 28 countries around the world. For more information, visit www.duffandphelps.com.

APPENDIX

NetDiligence® 2018 Cyber Claims Study

SMEs approx. 87%





Cyber insurance in a time of crisis

- All budgets must be approved by the carrier
- Excessive charges may not be covered
- May not cover additional proactive services
- Zurich refusing to pay NotPetya ransomware bill declaring it an “Act of War”