



CYBER RISK



READINESS



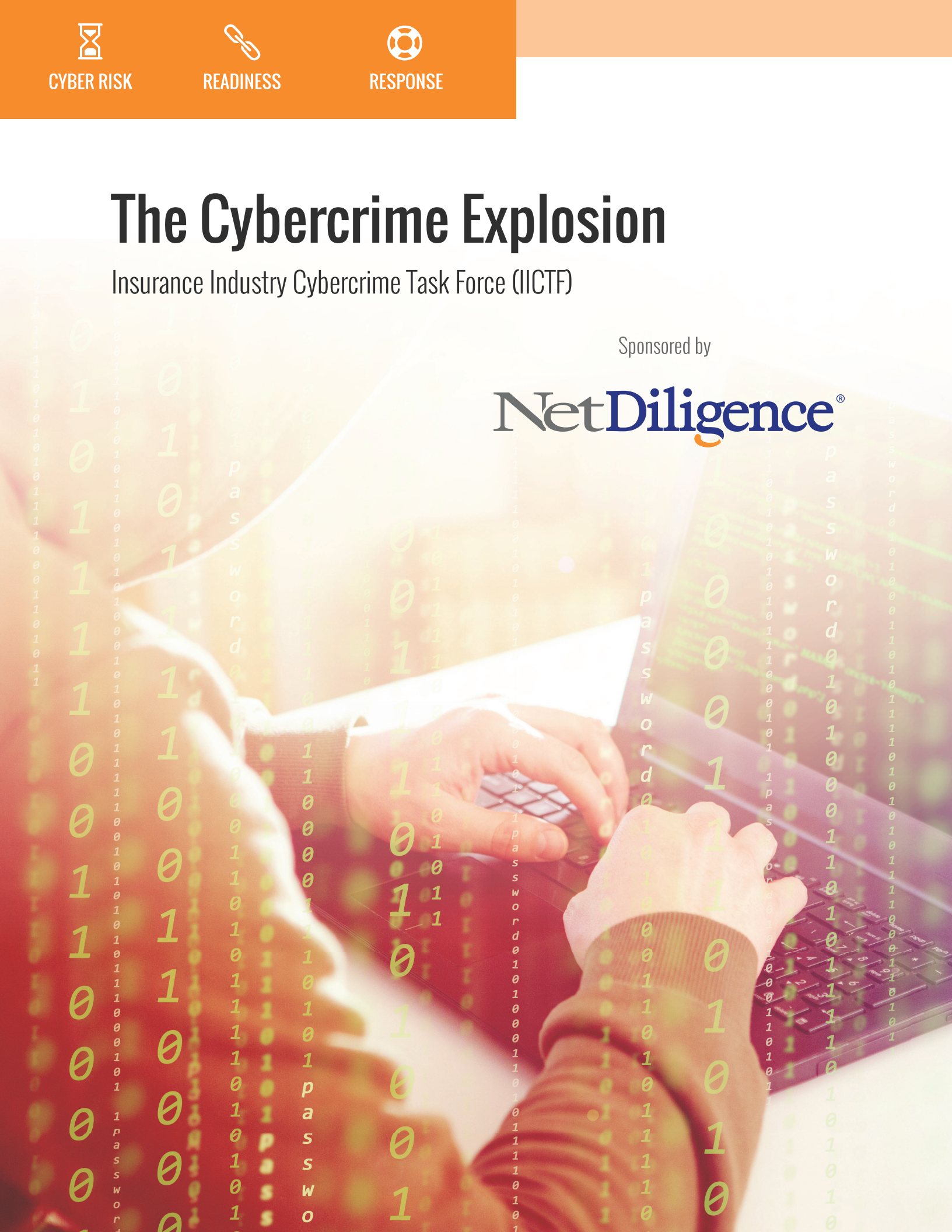
RESPONSE

The Cybercrime Explosion

Insurance Industry Cybercrime Task Force (IICTF)

Sponsored by

NetDiligence[®]



The Cybercrime Explosion

Insurance Industry Cybercrime Task Force (IICTF)

Introduction

No matter which study you read or which metric you use, the trend in cybercrime is incontrovertible: a dangerously steep upward trajectory. Cybercrime, attack vectors, and monetary loss have all grown substantially in the past few years. The potential for consequential damages from cybercrime is also growing at a rapid pace: loss of productivity, revenue and property; loss of trust; decline in share value; and the cost of updating equipment, software, and training.

The Insurance Industry Cybercrime Task Force (IICTF), sponsored by NetDiligence®, was formed in 2018 for the purpose of collecting, organizing, and reporting on cybercrime activity from the vantage point of cyber insurance, forensic response firms, legal/Breach Coach®, technology and law enforcement. Insurers, as well as the panel partners with whom they work, handle thousands of cyber-related claims each year and have first-hand experience analyzing and remediating these events. Consequently, the industry is uniquely positioned to provide valuable insight about cyber security risks, threats, and vulnerabilities. The opportunity exists to leverage their combined expertise to enhance our national efforts in the fight against cybercrime.

Participants in the task force include members of leading cyber insurance, legal and cybersecurity technology companies. The primary objective of the task force is to identify the cybercrimes that are impacting businesses in the United States and to collaborate with law enforcement and technology companies on ways to reduce criminal activity.

According to the 2018 Cyber Claims Study from NetDiligence¹, 274 criminal incidents in 2017 cost over \$160M, with an average cost of \$584K per incident. Estimates from task force participants suggest that in 2017, the aggregate cost of cybercrime events for companies with cyber insurance ranged from \$750M to \$900M. Since cyber insurance coverage typically excludes soft costs like customer loss, brand damage, and stock devaluation, our numbers represent a lower estimate of the actual costs of these criminal attacks. In addition, many incidents go unreported, and most companies do not have cyber insurance protection, so these numbers are just the tip of the iceberg.

In this paper we detail the top business sectors susceptible to criminal cyberattacks, the top causes of loss, and the costs associated with these incidents.

We believe that understanding where the attacks are coming from, where organizations are vulnerable, and how expensive incidents can be, are the first steps to protecting a company's assets, their customers and their reputation.

¹ 2018 Cyber Claims Study, NetDiligence®; November, 2018

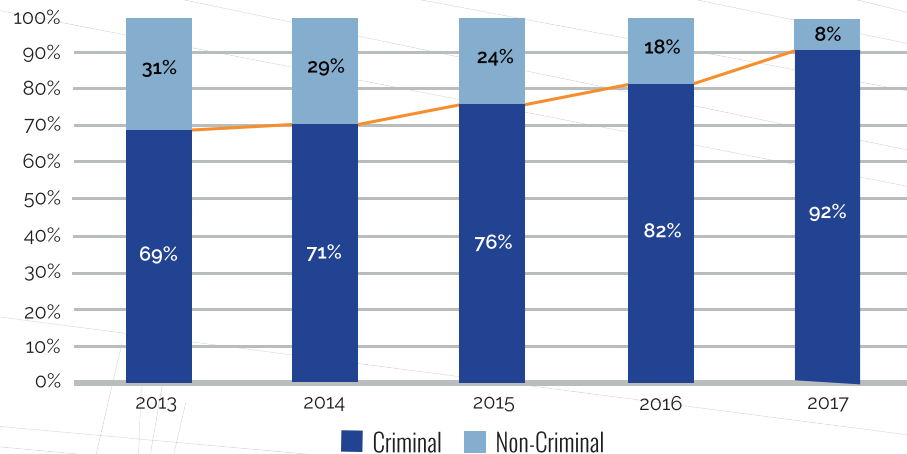
The Numbers

Estimates of the cost of cybercrime in 2016 and 2017—both in the US and globally—vary greatly, from \$17 billion to \$600 billion. The Herjavec Group has projected that the global cost of cybercrime will be \$6 trillion by 2021. Regardless of the estimates, the financial impact upon victim businesses can be devastating.

Professional services, healthcare, financial services, and retail are the business sectors with the highest frequency of cyber claims. Ransomware, hacking, malware, and business email compromises /phishing /social engineering are the top causes of cybercrime losses.

The average number of claims related to criminal activity processed by each of our task force insurance participants was 1,250 in 2017. Research from the NetDiligence Cyber Claims Study found that the proportion of cyber claims that is attributable to criminal activity has risen steadily from 69% in 2013 to 92% in 2017².

Criminal vs Non-Criminal
Percentage of Claims



Troubling Trends

The increase in cybercrime tracks closely with a growing variety of attack vectors. Businesses used to be attacked in order to gain customer credit card information for use or resale. Now the victim businesses themselves, perceived to be more profitable targets, have also become a focus. Attacks on businesses are designed to gain access to business data for exploitation or to deny the company access to their own files in order to force payment of a ransom to unlock the data. The NetDiligence study showed the top cybercrime-related causes of loss in 2017 were:

- Ransomware - 31%
- Business email compromise/social engineering/phishing - 24%
- Hacking - 19%
- Malware/Virus - 11%

² 2018 Cyber Claims Study, NetDiligence®; November, 2018

Evolving Ransomware Attacks

The number of ransomware events has increased dramatically since the beginning of 2017, with significantly higher costs. The higher costs appear to be resulting from more sophisticated malware which presents more challenges in data recovery. The following are additional troubling ransomware trends:

- Banking Trojans now “pre-qualify” victims to ensure six (6)-figure ransom payouts.
- “Demands of \$250,000 to \$500,000 were nonexistent six months ago and now they’re a weekly occurrence.” (Winston Krone, Global Managing Director, Kivu)³
- “Around midyear, top payouts in corporate ransomware attacks began to exceed \$1M, dwarfing the previous maximum of about \$17,000.” (Michael Tanenbaum, Executive Vice President, Chubb)⁴

In the past 12 months, there has also been a significant increase in more sophisticated ransomware attacks. In particular, Ryuk and BitPaymer ransomware variants have greatly increased in the past six months. In a Ryuk or BitPaymer attack, the following generally occur:

- An email carrying a malicious payload is opened by the recipient
- The network is infected with the malware Emotet or Trickbot, which belong to banking malware families and have numerous capabilities, such as credential harvesting, clipboard data harvesting, and the ability to pull down numerous modules capable of a range of other malicious activity
- Utilizing stolen credentials, the attackers access the system through RDP, VPN, or other means
- The attackers find and delete/encrypt backups, move throughout the system, and deploy encryption
- Demands are usually much higher – starting at 20 bitcoins (currently about \$80,000)

Other kinds of fraud occur concurrently, such as access to banking sites, AmazonPayPal, etc., using credentials gathered via Emotet and Trickbot.

- Emotet and Trickbot infections are also persistent and constantly changing. They can self-replicate, avoid detection, and usually require an advanced endpoint monitoring solution, or network rebuild, to contain.
- The attacks are often more targeted. The attackers seem to learn about their victim and adjust their price accordingly. There may also be different attack groups carrying out different phases of the attack. Initial access may be obtained by one group which then sells or trades access to another group.

³ *Bitcoin Intensifies Pain for Some as Ransom Demand Skyrockets*; Sonali Basak and Jennifer Surane, December 2017.

⁴ *Bitcoin Intensifies Pain for Some as Ransom Demand Skyrockets*; Sonali Basak and Jennifer Surane, December 2017.

Increasing Business Email Compromise (BEC) Attacks

In the past 12 months, there has also been a continued increase in Office 365/email account compromises. These attacks typically focus on redirecting funds and/or monetizing data in an email account.

Attacks that focus on the redirection of funds often target an executive or employee working in financial services. These attacks mine the data in a compromised email account for the purpose of redirecting wire transfer information.

Businesses with employee portals are often victims of email account compromises in which employee login credentials are harvested, allowing the malicious actor to access the portal, change direct deposit information, and redirect the payroll.

Similarly, businesses with member portals—such insurance or investment companies—are targeted for portal user credentials so the malicious actors can access the portal to cash out policies or investments and transfer the funds to their own accounts.

Email accounts are also compromised for the purpose of obtaining and monetizing the sensitive data in them. Email compromises can be costly, intrusive, and have a much greater impact on the business than other types of attacks.

Business Sectors

Parity among victimized industries is increasing, although sectors having the most sensitive data are still the biggest targets. Thus, while cybercrime has affected companies in every industry sector, healthcare and professional services were the top targets in our study:

- Professional services – 23%
- Healthcare – 15%
- Financial services – 11%
- Retail – 11%

Although one should not place too much emphasis on an individual company's book of business, one insurance company task force participant reported that 67% of the claims it processed were healthcare-related.

Financial Impact

While estimates of the financial impact of cybercrime, both now and in the future, vary broadly, the upward trend is unmistakable. No matter the source of the data, the clear conclusion is that claims and losses will increase:

- According to our study, the cost to insurers for cybercrime-related incidents in 2017 was estimated to be between \$600M-\$900M. Total breach costs were estimated to be between \$800M-\$1.2B. If we project these numbers to include cyber losses incurred by uninsured companies, estimated 2017 cyber losses in the US is between \$17B-\$120B.⁵

⁵ IICTF member estimates using data from NetDiligence® and other insurance sources.

- A report from the Council of Economic Advisers estimated \$57B-\$109B in US cyber-related losses in 2016.⁶
- A report published by McAfee and the Center for Strategic and International Studies estimated global losses due to cybercrime to be between \$445B and \$600B in 2017.⁷
- A report from Herjavec Group estimates that by 2021, cybercrime will cost the global economy \$6 trillion.⁸

Whatever estimate one elects to use, there can be no doubt that cybercrime is imposing a heavy financial burden on the United States and global economies.

Vulnerabilities

Cyber criminals rely on both human and technological vulnerabilities. While social engineering schemes have become more sophisticated, the task force members also reported that there have been some common technologies that are being exploited by savvy criminals. The following are common vulnerabilities utilized by cybercriminals to compromise email accounts and computer networks:

- Dormant/unnecessary ports and service accounts
- Systems that have not deployed multi-factor authentication
- Out of date security patches
- Lack of data protection – lack of encryption and/or lack of data inventory resulting in lack of protection due to unknown location and amount of sensitive data

Attribution

Attacks that focus on the redirection of funds often target an executive or employee working in financial services. These attacks mine the data in a compromised email account for the purpose of redirecting wire transfer information.

Attribution is difficult to ascertain. Regarding email account compromises, forensics firms report that phishing attacks for Office 365 account credentials tend to be associated with organized crime, much of it based out of, or using servers based out of, Nigeria and Russia.

Similarly, some ransomware is reportedly associated with organized crime, and federal law enforcement is actively investigating the creators and purveyors of certain ransomware variants. Some published material suggests that the group responsible for Ryuk ransomware may be affiliated with North Korea. Also, two Iranians were recently indicted for the SamSam attacks – though it is not clear whether they have ties to the government.

⁶ *The Cost of Malicious Cyber Activity to the US Economy*; The Council of Economic Advisors, February 2018

⁷ *Economic Impact of Cybercrime – No Slowing Down*; McAfee and CSIS, February 2018

⁸ *2017 Cybercrime Report*; Herjavec Group and Cybersecurity Ventures, date of publication unknown

Commonly seen IP addresses associated with both email compromises and ransomware attacks are based in Russia and Eastern Europe. Nigeria is also commonly associated with email compromises and system intrusions, especially those involving tax return software. China, Iran, Brazil, and Netherlands IP addresses are also frequently associated with cybercrime. Of course, IP addresses do not necessarily identify the true source or geographic location of an attacker.

Assigning attribution for criminal incidents is not standard practice in the insurance industry. Some IICTF participants tended to view criminal claims as either first or third party, with little regard for who caused the incident. Other participants, however, were interested and able to assign attribution in 50% or more of cases. In these matters, the following appeared to be the appropriate attribution:

- State Sponsored – 1%
- Organized Crime – 20%
- Hactivist – 49%
- Opportunistic – 30%

While criminal organizations are consistently after valuable data, including personal information, protected health information, credit card data, financial information, intellectual property, trade secrets, and anything else that can be resold, it is also important to realize that an increasing number of events (ransomware, DDoS and network outages) are “recordless” events that do not involve the exposure or theft of data, but are committed with the intent to extort the owner of operational data and cripple the victimized organization’s business operations.

Methodology

This report has been compiled from a variety of sources, including structured interviews with members of the IICTF who represent insurers that provide cyber insurance coverage, recognized incident response organizations, legal advisors who specialize in cyber insurance and data breach matters, and technologists who provide products in the cyber security and cyber insurance space.

In addition, data have been cited from public sources, including the 2018 Cyber Claims Study from NetDiligence and internal IICTF member projections and estimates.

Task Force Members



Jeremy Barnett
NAS Insurance



Winston Krone
Kivu



Jennifer Coughlin
Mullen Coughlin



Shawn Melito
Kivu



Tony Dolce
Chubb



Heather Osborne
NetDiligence



Ed Finn
Mullen Coughlin



Brian Robb
CNA



Sean Hoar
Lewis Brisbois



Phil Rosace
Guidewire



Doug Howard
RSA



Vinny Sakore
NetDiligence



Robert Jones
AIG

Contact Us

For more information about the IICTF, or if you have questions regarding the information presented in this report, please contact us at iictf@netdiligence.com.

About Our Sponsor

NetDiligence® specializes in Cyber Risk Readiness & Response services. With more than 15 years of experience in cyber, NetDiligence is an award-winning provider of innovative cyber risk management software and services to the insurance industry, including [QuietAudit®](#), [Cyber Risk Assessments](#), the [eRiskHub®](#) cyber risk management portal, and [Breach Plan Connect®](#) software-as-a-service (SaaS) that helps companies develop an effective data breach response plan. NetDiligence publishes an annual [Cyber Claims Study](#) and hosts annual [Cyber Conferences](#) in Philadelphia, Santa Monica, Toronto, London and Bermuda. For more information, visit NetDiligence.com.