**LITERATURE SURVEY**

1. **“Chronology of Data Breaches”.**

**AUTHORS: P. R. Clearinghouse** .

Data breaches have gained widespread attention as businesses of all sizes become increasingly reliant on digital data, cloud computing, and workforce mobility. With sensitive business data stored on local machines, on enterprise databases, and on cloud servers, breaching a company’s data has become as simple – or as complex – as gaining access to restricted networks.

Data breaches didn’t begin when companies began storing their protected data digitally. In fact, data breaches have existed for as long as individuals and companies have maintained records and stored private information. Before computing became commonplace, a data breach could be something as simple as viewing an individual’s medical file without authorization or finding sensitive documents that weren’t properly disposed of. Still, publicly-disclosed data breaches [increased in frequency in the 1980s](http://searchsecurity.techtarget.com/feature/Data-breach-protection-requires-new-barriers), and in the 1990s and early 2000s, public awareness of the potential for data breaches began to rise.Laws and [regulations such as HIPAA](https://digitalguardian.com/blog/what-hipaa-compliance) or the [PCI Data Security Standard](https://digitalguardian.com/blog/what-pci-compliance) are created to provide guidelines for companies and organizations handling certain types of sensitive consumer information. These regulations provide a framework for the required safeguards, storage, and use practices for handling sensitive information, but these rules don’t exist in all industries, nor do they definitively stop data breaches from occurring.

# 2)“ Finds New Report From Identity Theft Resource Center and CyberScout.,”.

# AUTHORS: ITR Center. Data Breaches Increase 40 Percent in 2016

# Breaches involving accidental email/internet exposure of information was the second most common type of breach incident at 9.2 percent of the overall number of breaches followed by employee error1 at 8.7 percent. With the exception of hacking, all other categories reflected decreases from 2015 figures."For businesses of all sizes, data breaches hit close to home, thanks to a significant rise in CEO spear phishing and ransomware attacks. With the click of a mouse by a naïve employee, companies lose control over their customer, employee and business data. In an age of an unprecedented threat, business leaders need to mitigate risk by developing C-suite strategies and plans for data breach prevention, protection and resolution," said Matt Cullina, CEO of CyberScout and Vice Chair of ITRC's Board of Directors.Since 2010, the ITRC has been tracking breaches involving Social Security numbers (SSNs) and credit card/debit card numbers. Exposure of SSNs was evidenced in 52.0 percent of the overall number of breaches in 2016, representing an increase of 8.2 percent over 2015 figures. Exposure of records involving credit/debit cards at 13.1 percent, reflects a decrease of 7.4 percent from 2015. With that said, it is important to remember that most data breach notifications or media reports do not include the type of information exposed. The spike in SSN exposures is in clear alignment with the surge of CEO spear phishing attacks, which target this type of information.Adam Levin, Chairman and Founder of CyberScout, said, "The database compromises of 2016 confirmed yet again that breaches are the third certainty in life and we are all living in a constant state of cyber insecurity. Hackers and identity thieves continue to evolve. They are very sophisticated, extremely creative and dogged in their pursuit of what is ours. More than half of the breaches reported by the ITRC included the skeleton key to our lives: the Social Security number. This trend, which has accelerated since 2015— when just four breaches exposed over 120 million Social Security numbers to state-sponsored hackers and cyber criminals— represents the point of no return for millions of Americans. While credit and debit card numbers can be changed, SSNs cannot. Therefore, monitoring and damage control become even more important than ever before. Consumers must become better informed as to the risks inherent in this dangerous digital world, be more alert to the signs of individual compromise and know what to do to contain and reverse the damage or take advantage of identity theft protection services offered by their insurers, employers or financial services firms."

# 3) “Cybersecurity Incidents.,”.

# AUTHORS : C. R. Center****.****

# [yber Security](https://www.lawinsider.com/dictionary/cyber-security-incident) Incident means any thing, event, act or omission which gives, or may give, rise to: unauthorised access to any information system, data or electronic communications network (including breach of an applicable security policy); reduced integrity of an information system, data or electronic communications network; unauthorised use of any information system or electronic communications network for the processing (including storing) of data; disruption or change of the operation (including, but not limited to, takeover of control, malicious disruption and/or denial of service) of an information system or electronic communications network; unauthorised changes to firmware, software or hardware; unauthorised destruction, damage, deletion or alteration of data residing in an information system or electronic communications network; removal or limiting the availability of, or possibility to use, data residing in an information system or electronic communications network; the appropriation, publication, dissemination or any other use of data by persons unauthorised to do so; or a breach of the Computer Xxxxxx Xxx 0000, the Network and Information Systems Regulations 2018, the UK GDPR or the Data Protection Xxx 0000, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Communications Xxx 0000, the Official Secrets Xxx 0000 to 1989, or any other applicable legal requirements in connection with cybersecurity and/or privacy in connection with the Services and/or this Contract; Guidance notes: Please note that the Privacy and Electronic Communications (EC Directive) Regulations 2003 are planned to be replaced with new legislation in the future

# 4) “What do we know about cyber risk and cyber risk insurance,”

**AUTHORS: M. Eling and W. Schnell**

**Purpose**

This paper aims to provide an overview of the main research topics in the emerging fields of cyber risk and cyber risk insurance. The paper also illustrates future research directions, from both academic and practical points of view.

### **Design/methodology/approach**

The authors conduct a literature review on cyber risk and cyber risk insurance using a standardized search and identification process that has been used in various academic articles. Based upon this selection process, a database of 209 papers is created. The main research results findings are extracted and organized in seven clusters.

### **Findings**

The results illustrate the immense difficulties to insure cyber risk, especially due to a lack of data and modelling approaches, the risk of change and incalculable accumulation risks. The authors discuss various ways to overcome these insurability limitations, such as mandatory reporting requirements, pooling of data or public–private partnerships in which the government covers parts of the risk.

### **Originality/value**

Despite its increasing relevance for businesses at present, research on cyber risk is limited. Many papers can be found in the IT domain, but relatively little research has been done in the business and economics literature. The authors illustrate where research stands currently and outline directions for future research.

# 5) “Heavy-tailed distribution of cyber-risks”.

# AUTHORS: T. Maillart and D. Sornette.

# With the development of the Internet, new kinds of massive epidemics, distributed attacks, virtual conflicts and criminality have emerged. We present a study of some striking statistical properties of cyber-risks that quantify the distribution and time evolution of information risks on the Internet, to understand their mechanisms, and create opportunities to mitigate, control, predict and insure them at a global scale. First, we report an exceptionnaly stable power-law tail distribution of personal identity losses per event, Pr(ID loss ≥ V) ~ 1/Vb, with b = 0.7 ± 0.1. This result is robust against a surprising strong non-stationary growth of ID losses culminating in July 2006 followed by a more stationary phase. Moreover, this distribution is identical for different types and sizes of targeted organizations. Since b < 1, the cumulative number of all losses over all events up to time t increases faster-than-linear with time according to ≃ t1/b, suggesting that privacy, characterized by personal identities, is necessarily becoming more and more insecure. We also show the existence of a size effect, such that the largest possible ID losses per event grow faster-than-linearly as ~S1.3 with the organization size S. The small value b ≃ 0.7 of the power law distribution of ID losses is explained by the interplay between Zipf’s law and the size effect. We also infer that compromised entities exhibit basically the same probability to incur a small or large loss.