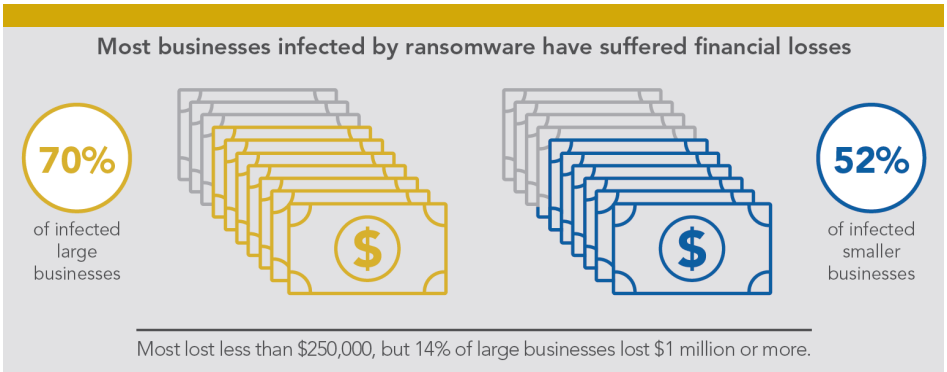
Executive Summary

USI 2017 Cybersecurity and Data Privacy Study:

Decision-makers Report Shifting Concerns, Escalating Risks

More companies are expanding information technology budgets, purchasing insurance, and developing incident response and business continuity plans to address the increasing complexity and frequency of cybersecurity and data privacy incidents, according to USI's 2017 Cybersecurity and Data Privacy Study.



The study shows the top concern for large businesses, companies with $100 million or more in annual revenue, shifted in 2017 from leaking or loss of private data to managing reputation and regulatory risks. For smaller businesses, firms with $5 million to under $100 million in annual revenue, leaking of private data remains the primary concern.

The difference in concern levels may be because smaller businesses don't have the resources to respond to private data leaks, according to USI's cybersecurity and privacy experts.

Based on a survey of 200 decision-makers, equally representing large and smaller companies, the study provides unique insights into trends and perceptions of cybersecurity and data privacy vulnerabilities, the challenges companies face when reviewing their exposures, the prevalence of impostor fraud and ransomware, and plans for dealing with business interruption due to virus or denial of service attack.

Incident and Claims Experience

While large businesses are more likely to experience a data privacy incident and ransomware attack, the survey showed theft of portable devices or hard drives by someone external to the organization was more likely to occur at smaller businesses.

Of the survey participants representing smaller firms, 32% reported experiencing a data privacy incident in the past year, 25% reported being targeted by ransomware, and 32% confirmed having been a target of impostor fraud.

Large businesses that were the target of impostor fraud in the past year experienced a financial loss of between $100,000 and $500,000, according to the survey. Smaller business losses from impostor fraud ranged from $25,000 to less than $250,000. While smaller businesses were less likely to have been targeted, half of the targeted businesses reported suffering monetary loss.

Cyber extortion and ransomware attack losses were under $250,000 for a majority of survey participants. About 14% of large businesses indicated their losses were more than $1 million.

Insurance and Risk Management

The survey showed organizations are adding cybersecurity and data privacy coverage to their insurance portfolio as they realize the risks inherent in the collection of employee records and the increased reliance on computer networks.

According to the survey, the majority of smaller businesses (82%) reported purchasing cybersecurity and data privacy risk insurance to protect from financial loss and 74% cited preparing for a data privacy breach as their top reason for buying the coverage.

Less than half of smaller businesses have purchased impostor fraud coverage as part of their insurance portfolio – this

is lower than the percentage of those smaller business that have business interruption insurance.

The survey also shows a majority of smaller businesses have evaluated the financial impact of a disruption from a virus or denial of service attack, yet 45% do not have network business interruption insurance.

Both large and small businesses face challenges when acquiring insurance to protect against cybersecurity and data privacy risks, according to the survey. For smaller businesses, finding policies that fit their unique needs was cited as the most significant challenge followed by cost of coverage. Notably, the survey shows 30% of smaller businesses are unsure of how to begin looking for cybersecurity and data privacy risk insurance.

For large businesses, cost was cited as the biggest challenge to obtaining insurance.

Compared to smaller firms, large businesses are more likely to have an incident response plan that has been tested and which they consider to be effective. The majority of large and smaller businesses reported having business continuity plans that have been tested.

How USI Can Help

The 2017 Cybersecurity and Data Privacy Study exposed significant businesses vulnerabilities when it comes to businesses protecting against cyberattacks and privacy risk threats. For example, it is clear that smaller businesses need to talk to their broker about adding insurance for impostor fraud – a confusing coverage that some mistakenly believe is covered by a typical crime policy. Also, fewer smaller companies have network business interruption insurance.

Many businesses that have an incident response plan have used it in the past 12 months.

Finally, companies of all sizes need a cyber risk assessment to identify the strengths and weaknesses in their data security plan and strategies for improvement. While purchasing cybersecurity and data privacy insurance is a solid step, it should be used in tandem with developing and testing a comprehensive incident response plan.

No matter what type of cyber incident, the consequences of a cybersecurity and data privacy breach to an organization of any size can be catastrophic. For some businesses the financial loss, including business interruption cost, can be in the millions of dollars and the reputational harm irreparable.

The experienced risk management professionals at USI Insurance Services have had tremendous success matching clients with the latest and most effective cyber and privacy risk solutions.

For customized risk transfer solutions and best practices, or a copy of the Cybersecurity & Data Privacy Study, please contact your USI representative or visit usi.com.

The USI ONE Advantage®

To analyze our client's business issues and challenges, our Cyber Risk team leverages USI ONE®, a fundamentally different approach to risk management. USI ONE integrates proprietary business analytics with a network of local and national technical experts in a team based consultative planning process to evaluate the client's risk profile and identify targeted solutions. Clients then receive tailored recommendations for improving their total cost of risk. To learn more about USI ONE and the USI ONE Advantage, contact your local USI team today.