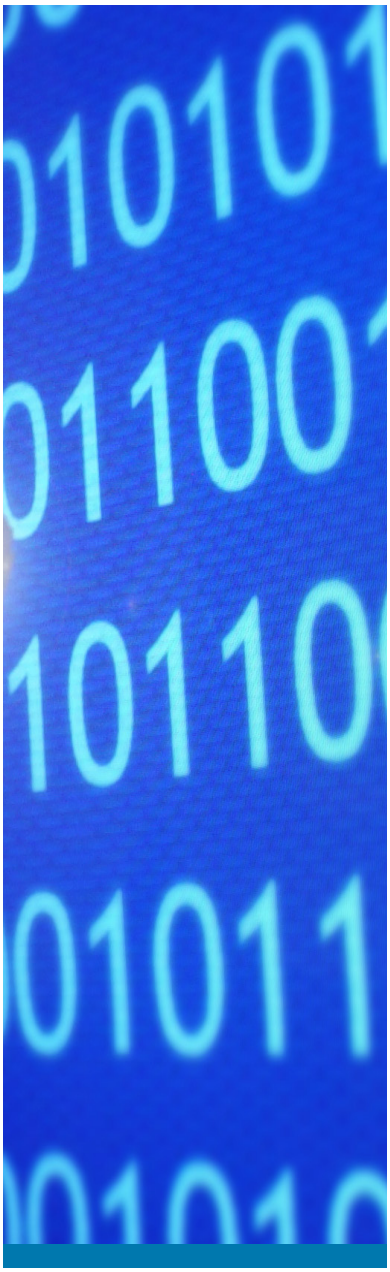
CASE STUDY: ROI ON CYBER RISK INSURANCE



CALCULATING THE VALUE OF CYBER RISK MANAGEMENT

EXECUTIVE SUMMARY

IMA interviewed the CFO of a national retailer that had no cyber risk insurance and recently became the victim of a data breach. The breach resulted from an email phishing ploy to get access to the point-of-sale systems within stores. The company was made aware of the event by its payment processor.

- 100,000 unique payment card records were stolen
- Total event expenses incurred: $2,900,000
- Company could have purchased cyber insurance for approximately one percent of the loss incurred

CHALLENGES

Upon discovering the breach, the company was nearly paralyzed as it went into crisis mode. It had no defined incident response plan nor designated vendors to assist with an investigation and strategy.

They were forced to identify and negotiate with vendors with zero leverage in a limited time frame. They also had to deal with an investigation, regulatory scrutiny and keep regular business operations intact. It was a potentially catastrophic event that occupied key stakeholders for more than a two-month period.

- Three IT employees were dedicated exclusively to investigation and remediation over six weeks.
- Point-of-sale systems were taken offline for five weeks during investigation, and the company had to manually process payments.
- The company was in the midst of a sale and buyer backed out due to unknown consequences.
- The company did eventually resolve the event; however, expenses came in at around $3,000,000 and they experienced unknown reputational damage.

CASE STUDY: ROI ON CYBER RISK INSURANCE

In today's world it is not a question of if, but when, a data security incident will happen.

Awareness and preparation are critical in minimizing the effects of an event.

Cyber insurance is now an essential part of corporate risk strategy.

HOW IMA COULD HAVE HELPED

IMA's team helps organizations go through the analysis of defining their unique operational cyber risk exposures.

Part of our cyber risk planning includes modeling the probable loss based on the volume and type of confidential information maintained. Loss modeling indicates the total potential cost of an event. IMA uses that amount as a suggested limit of coverage and then seeks insurance quotes from carriers able to meet the client needs. IMA also maintains a proprietary cyber risk loss control website. The site provides best practices, loss modeling and privacy training for all clients.

Because this company in particular did not have a defined incident response plan, we would have prioritized an insurance carrier that includes a breach management turnkey solution as part of their policy.

Specifically, once there was a suspicion of a breach the company could have had immediate access to a "breach coach." A breach coach is an attorney that specializes in data breach events and provides a triage function.

A breach coach's initial consultations are complimentary as part of most cyber risk policies. If after initial consultation there is a reasonable suspicion of a breach, a carrier can provide immediate access to all necessary service vendors to assist in efficiently managing the breach. These vendors are top-tier service firms—services are provided at a discount up to 40 percent based on the carrier's purchasing power.

IMA also provides a list of vendors to choose from so clients have the opportunity to interview and select service providers. Once the firms have been identified, they are incorporated into the incident response plan and policy. The policy is meant to be a seamless funding mechanism to cover obligations that arise from a data breach.

RETURN ON INSURANCE INVESTMENT

While the purchase of cyber insurance does not eliminate the possibility of a data breach, it provides timely access to experts to assist in the investigation and management of the crisis. It also decreases the expense, funds the loss and eases the burden on management.

Based on this organization's risk profile, we would have recommended a $3,000,000 policy. When compared to our peer benchmarking, this amounts to a premium of approximately $27,500.

**Chart for illustrative purposes. Results not guaranteed.*

Without Insurance		With Insurance		
Expense Item	**Actual Amount Incurred**	**Expense Item**	**Amount Incurred With Insurance Discount (where applicable)**	**Amount Covered**
Legal Counsel	$500,000	Legal Counsel	$300,000	$300,000
External Forensic Investigation	$700,000	External Forensic Investigation	$630,000	$630,000
Three Employees Exclusively Dedicated to Investigation for 3 Weeks	$72,000	Three Employees Exclusively Dedicated to Investigation for 3 Weeks	$72,000	$72,000
Public Relations Firm	$25,000	Public Relations Firm	$20,000	$20,000
Notification Costs	$5,000	Notification Costs	$4,500	$4,500
Credit Monitoring	$3,000	Credit Monitoring	$2,700	$2,700
PCI Fines & Penalties	$1,500,000	PCI Fines & Penalties	$1,500,000	$1,500,000
Lost Business	$90,000	Lost Business	$90,000	$90,000
TOTAL	**$2,895,000**	Annual Premium for $3M Limit	$27,500	$0
		Deductible	$25,000	$0
		TOTAL	**$2,671,700**	**$2,619,200**

BALANCE SHEET EVENT IMPACT (WITHOUT INSURANCE)

- ($2,895,000)

BALANCE SHEET EVENT IMPACT (WITH INSURANCE)

- Annual Premium: ($27,500)
- Deductible: ($25,000)
- Vendor Discounts: $276,000
- Insurance Recovery: $2,619,200

LESSONS LEARNED

- Immediate access to qualified service providers that can steer the process is critical.
- Training and planning to prepare for an event creates a more efficient process and decreased expense.
- A risk transfer solution can assist with coordination and funding of obligations.

In summary, effective cyber risk management helps mitigate loss but also provides a financial backstop in case of a catastrophic event.

"Clearly, avoidance was not a realistic strategy."

— CFO of national retailer

TO LEARN HOW TO MANAGE YOUR CYBER RISK, CONTACT:

Tim Burke
Director of Cyber Risk
IMA, Inc.
303.615.7676 | tim.burke@imacorp.com

www.imacorp.com/your-business/cyber-privacy-coverage