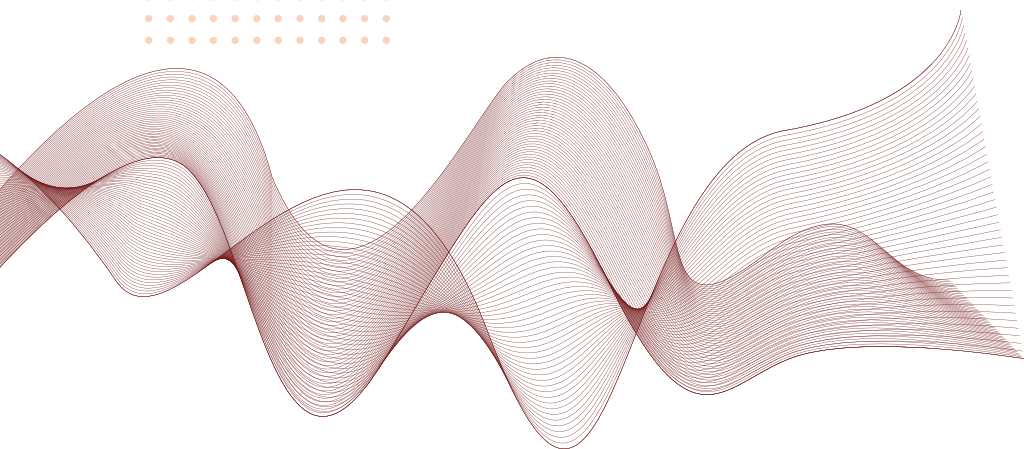


WHITE PAPER:

REPUTATIONAL LOSS

HOW TO SAFEGUARD YOUR
BUSINESS FROM CYBER
INCIDENTS IN THE AGE OF AI



JOSEPH SCARLATO, MBA, CFE

EVP, Global Technical Lead | Ampcus Forensics

INTRODUCTION

The Hidden Cost of a Cyberattack

Imagine for a moment:

You've meticulously built a trusted brand. You've poured all your heart, soul, and perhaps an unhealthy amount of caffeine into its growth. But then, one morning, you wake up to discover that your customer database has been hacked, exposing sensitive client information.

Panic ensues – and soon thereafter, outrage. Loyal customers start to abandon ship. Trusted partners treat you like you've got the plague. Your hard-earned reputation is now in tatters.

For some, this nightmare has been a lived reality. In an age where public perception is formed in real-time, an organization's response – and how long it takes – is critical to survival.

Financial losses can be measured, but reputational damage operates on a different scale – one that lingers long after the breach is patched. For organizations that have a plan, act swiftly, communicate transparently, and implement proactive recovery measures, however, it is possible to not only survive cyber incidents, but to emerge stronger on the other side.



Joseph Scarlato
EVP, Global Technical Lead
Ampcus Forensics

UNDERSTANDING REPUTATIONAL LOSS

Why is rebuilding trust so hard?

The consequences of reputational harm are far-reaching, extending well beyond immediate financial impacts. When customers lose faith in your ability to protect their data, rebuilding trust is no simple task—it requires strategic action, financial investment, and, most importantly, time.

HOW MUCH IS YOUR REPUTATION WORTH?

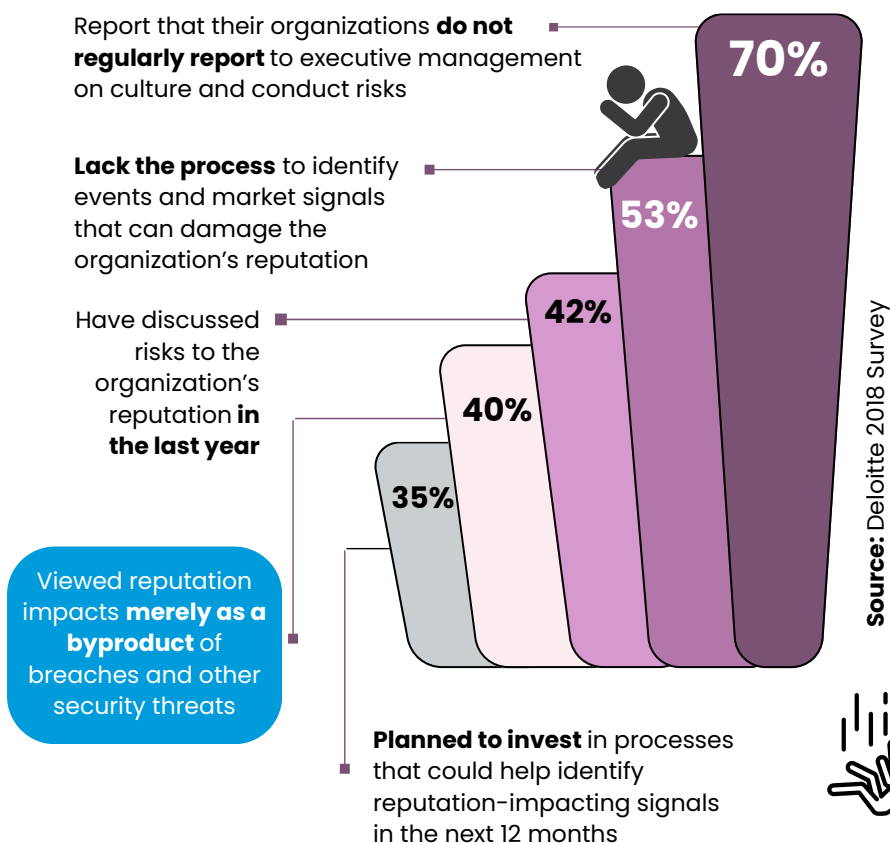


**IN 2020, WEBER SHANDWICK
SURVEYED 2,200 EXECUTIVES
AND FOUND THAT REPUTATION
ACCOUNTS FOR MORE THAN
63% OF A COMPANY'S
MARKET VALUE.**

Loss of Customer Trust

A cyber incident can turn even the most loyal customers into skeptics overnight. And when personal or financial information is compromised, people don't just shrug it off — they take their business elsewhere.

In some industries, even a small percentage of lost customers can mean millions in lost revenue. The longer a breach remains unaddressed, the greater the likelihood that businesses will struggle to recover their customer base.



Negative Media Coverage

If there's one thing the media loves, it's a scandal. A cyberattack can quickly become front-page news, and without the right response, the narrative can spiral out of control. Delays in disclosure or attempts to downplay the situation only make things worse. **Companies that fail to manage their public image after a breach can see long-lasting damage**, with some businesses experiencing a decline in new customer acquisition for years after an incident.

Decreased Business Opportunities

It's not just customers who take notice—vendors, investors, and partners may also second-guess their relationships with an organization that has suffered a breach. **Contracts can be lost, deals can be pulled, and suppliers may impose stricter terms**, leading to increased operational costs. The financial consequences of these disruptions can be significant, sometimes exceeding the direct costs of the cyberattack itself.

Long-Term Brand Damage

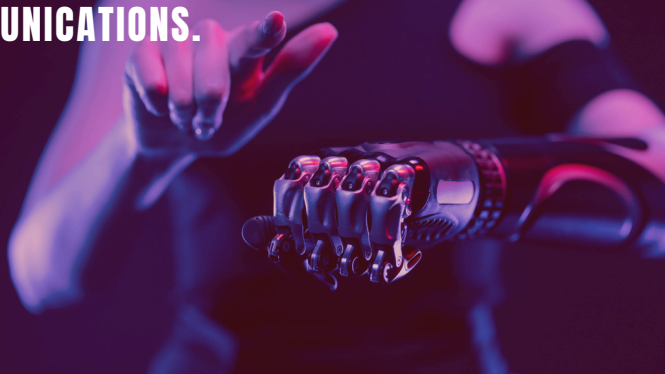
Rebuilding a reputation isn't as simple as issuing an apology and moving on. Businesses that suffer a cyber incident often need to invest heavily in **marketing, customer outreach, and brand rehabilitation** efforts just to get back to where they were before the breach. Some companies spend years—and substantial amounts of money—trying to restore confidence, and even then, the stigma can linger.

THE ROLE OF AI IN CYBER INCIDENTS

Artificial Intelligence is a double-edged sword in cybersecurity. On one hand, it's an incredibly powerful tool for identifying and mitigating threats **before** they cause damage. On the other, though, cybercriminals are using AI to expertly craft increasingly sophisticated attacks.

AI-DRIVEN THREATS

GONE ARE THE DAYS OF OBVIOUS SCAM EMAILS RIDDLED WITH TYPOS. AI-POWERED CYBERATTACKS NOW MIMIC EXECUTIVES' LANGUAGE, GENERATE FRAUDULENT INVOICES THAT LOOK LEGITIMATE, AND ADAPT IN REAL TIME TO BYPASS SECURITY MEASURES. SOME BUSINESSES HAVE LOST SIGNIFICANT SUMS BECAUSE EMPLOYEES COULDN'T DISTINGUISH AI-GENERATED FRAUD FROM REAL INTERNAL COMMUNICATIONS.



AI for Early Detection and Mitigation

Fortunately, AI is just as effective at playing defense as it is at offense. Modern AI-powered security tools can identify suspicious behavior in real time, stopping threats before they escalate. Businesses using these advanced systems can significantly reduce the time it takes to detect a breach—limiting damage before it spirals out of control.

AI-Enhanced Crisis Management

When a breach occurs, AI can also help manage the fallout. By analyzing public sentiment, businesses can anticipate how customers will react and tailor their response accordingly. AI-driven crisis management tools can help organizations regain control of the narrative, ensuring they respond in a way that restores trust rather than erodes it further.

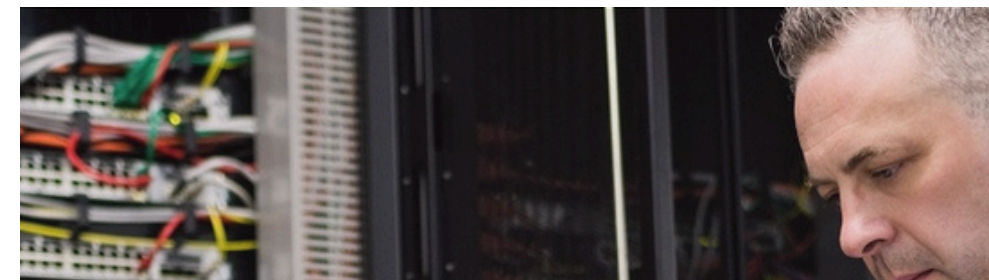
FORENSIC INSIGHT

Danielle M. Gardiner, CPA, CFF
Chief Forensics Officer:

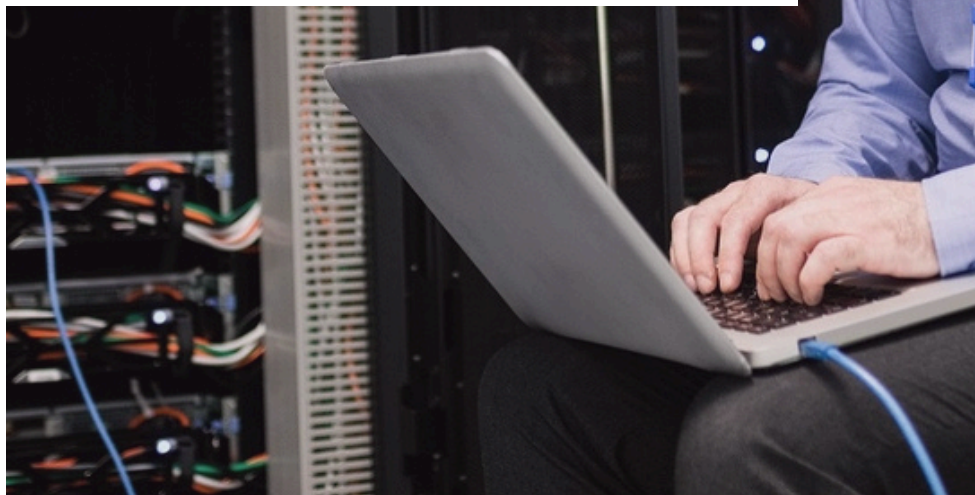
It's concerning that some companies fail to recognize the financial implications of reputational risk as it pertains to AI. Reputation directly affects revenue, and I urge risk management professionals to account for this when assessing and modeling current risk transfer strategies.



THE TRUE **COST** OF REPUTATIONAL LOSS



Cyber incidents don't just cause a short-term financial hit—they have long-term consequences that ripple across an organization.



Businesses that experience major breaches often face:

Customer churn and lost revenue

Even a small percentage of lost customers can translate to massive financial losses.

Brand damage and market share loss

Rebuilding consumer confidence requires significant marketing efforts and time.

Operational disruption

Downtime and lost productivity following an attack can strain a company's bottom line.

Legal and regulatory penalties

Fines for non-compliance can reach staggering amounts depending on the severity of the breach.

After the Cambridge Analytica Scandal,



THE FTC FINED FACEBOOK

\$5 BILLION

**FOR BAD PROCESSING
PRACTICES OF USERS' DATA.**

REPUTATION HAS ALWAYS MATTERED



But expectations change.



90% of respondents surveyed said corporate reputation was a primary asset (**The Economic Intelligence Unit, 2005**)



87% of executives rate reputation risk as more critical than other risks (**Deloitte Global Survey on Reputation Risk, 2014**)



86% of respondents said the loss of income, reduced customer base was the greatest impact of reputation risk (**WTW Global Reputational Risk Management Survey Report, 2021**)

In the age of AI, social media and instant access, consumer sentiment is felt **and shared** in real-time, sometimes to disastrous results for the business.

STRATEGIES TO RESTORE TRUST & MITIGATE REPUTATIONAL DAMAGE

When a cyber incident occurs, containing the damage, restoring public confidence, and supporting long-term recovery is essential. Key steps include:

#1 Incident Response & Transparent Communication

The faster a company acknowledges and addresses a breach, the better. Organizations that act quickly and communicate clearly can minimize reputational harm, while those that delay risk a permanent loss of trust. Incident response efforts can be costly, but they pale in comparison to the long-term damage of mishandling a crisis.

#2 Customer Support and Remediation Services

Providing affected customers with identity theft protection, credit monitoring, and direct support shows that a business takes their security seriously. These services come at a cost, but they are an essential investment in rebuilding trust.

#3 Legal and Regulatory Compliance Guidance

Every jurisdiction has its own rules regarding data breaches, and failing to follow them can result in hefty fines. Ensuring compliance not only mitigates legal risk but also reassures the public that the company is taking the necessary steps to protect its customers.

#4 Public Relations and Media Management

A well-crafted public response can mean the difference between a temporary setback and a permanent reputational stain. Companies that proactively manage their messaging and engage with customers transparently can significantly improve their chances of recovering from an incident.

#5 Enhanced Security Solutions for Long-Term Protection

The best way to mitigate reputational loss? Prevent the breach from happening in the first place. Investing in AI-driven monitoring, multi-factor authentication, and employee training can drastically reduce the likelihood of an attack.

NOT ALL INCIDENTS ARE CREATED – OR HANDLED – EQUALLY



A data breach sounded the death-knell on a failing business model and sent 23andMe into bankruptcy.



CrowdStrike has been able to claw back **\$30B** in losses – and largely repair its reputation – from a data incident that caused massive outages.

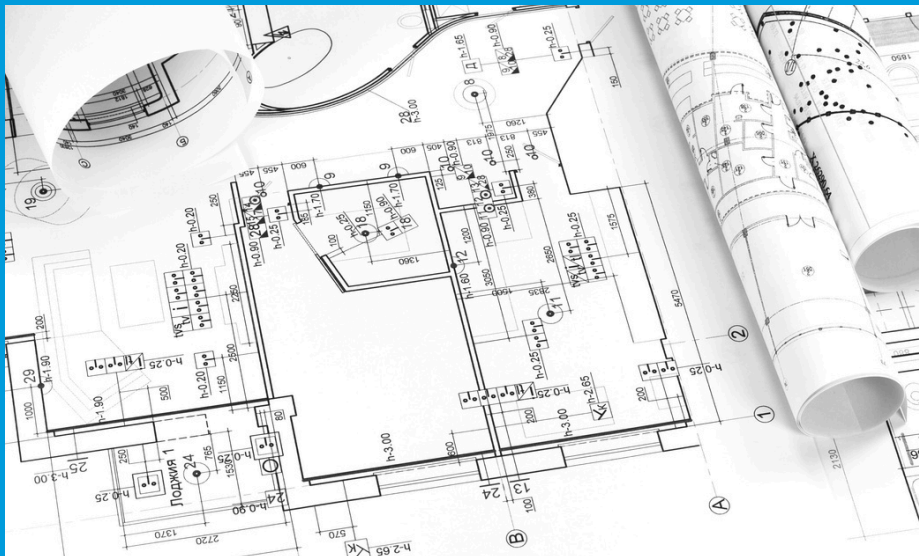


Boeing's refusal to pay a \$200m ransomware demand caused major outages but they remain a major defense and space contractor.



The 2024 breach cost them over **\$27m** in expenses, **\$18.9m** in revenue and resulted in an **\$86m** class-action settlement.

CONCLUSION



Turning Crisis into Opportunity

A cyber incident may feel catastrophic, but it doesn't have to spell disaster. Businesses that respond swiftly, communicate transparently, and take decisive action to restore trust can emerge stronger than before.

At **Ampcus Forensics**, we specialize in guiding businesses through the recovery process, ensuring they don't just rebuild their reputation but reinforce it. By prioritizing communication, proactive customer care, and security enhancements, organizations can minimize the long-term impacts of cyber incidents and confidently restore their reputation.

SOURCES:

- **WEBER SHANDWICK**

- [THE STATE OF CORPORATE REPUTATION IN 2020: EVERYTHING MATTERS NOW](#) | **KRC RESEARCH**

- **DELOITTE**

- [GLOBAL RISK MANAGEMENT SURVEY, 12TH EDITION](#)
- [REPUTATION @T RISK \(OCT 2014\)](#)

- **FEDERAL TRADE COMMISSION**

- [FTC IMPOSES \\$5 BILLION PENALTY AND SWEEPING NEW PRIVACY RESTRICTIONS ON FACEBOOK](#) | **FTC CHAIRMAN JOE SIMONS, FTC COMMISSIONERS NOAH JOSHUA PHILLIPS AND CHRISTINE S. WILSON AND DIRECTOR OF THE DEPARTMENT OF JUSTICE CIVIL DIVISION'S CONSUMER PROTECTION BRANCH GUSTAV W. EYLER.**

- **NATIONAL LAW REVIEW**

- [OCC ELIMINATES "REPUTATIONAL RISK" CATEGORY FROM BANK SUPERVISION CRITERIA](#) | **A.J. S. DHALIWAL, MEHUL N. MADIA, BEINENG ZHANG - SHEPPARD, MULLIN, RICHTER & HAMPTON LLP**

- **THE ECONOMIC INTELLIGENCE UNIT**

- [ORGANISATIONAL AGILITY: HOW BUSINESS CAN SURVIVE AND THRIVE IN TURBULENT TIMES](#) | **EMC**

- **WILLIS TOWERS WATSON**

- [WTW GLOBAL REPUTATIONAL RISK MANAGEMENT SURVEY REPORT, 2021](#) | **KEVIN VELAN**

- **SECURE FRAME**

- [15 RECENT CYBER ATTACKS & WHAT THEY TELL US ABOUT THE FUTURE OF CYBERSECURITY](#) | **ANNA FITZGERALD, ROB GUTIERREZ**



DANIELLE M. GARDINER, CPA, CFF
Chief Forensics Officer
Providence, RI | [LinkedIn](#)



JOSEPH SCARLATO, MBA, CFE
EVP, Global Technical Lead
Washington, DC | [LinkedIn](#)



CARLOS A. RIVERA, CFE, MACC
Senior Vice President
Miami, FL | [LinkedIn](#)



GRANT MIZEL, MBA, CFE
Senior Manager,
Forensic Accountant
Washington, DC | [LinkedIn](#)



CHRISTOPHER T. CERRINA
Forensic Accountant
Atlanta, GA | [LinkedIn](#)

WHO WE ARE

Ampcus Forensics is a boutique forensic accounting practice that offers clients decades of experience, white-glove service and AI automation solutions to resolve claims fast and keep business moving forward.

From complex litigation matters to fraudulent insurance claims, our client-centric approach and tailored service experience includes:



Business Interruption



Fraud Investigations



Litigation Support



Fee Fund Accounting



TPA Portfolio Review



Risk Management Consulting

We serve global clients across multiple industries, with specialties in Energy, Healthcare, Hospitality, Insurance, Manufacturing, Mining, Nonprofits, Oil & Gas, Renewables, Retail, Technology and Utilities.

Learn more at www.ampcusforensics.com