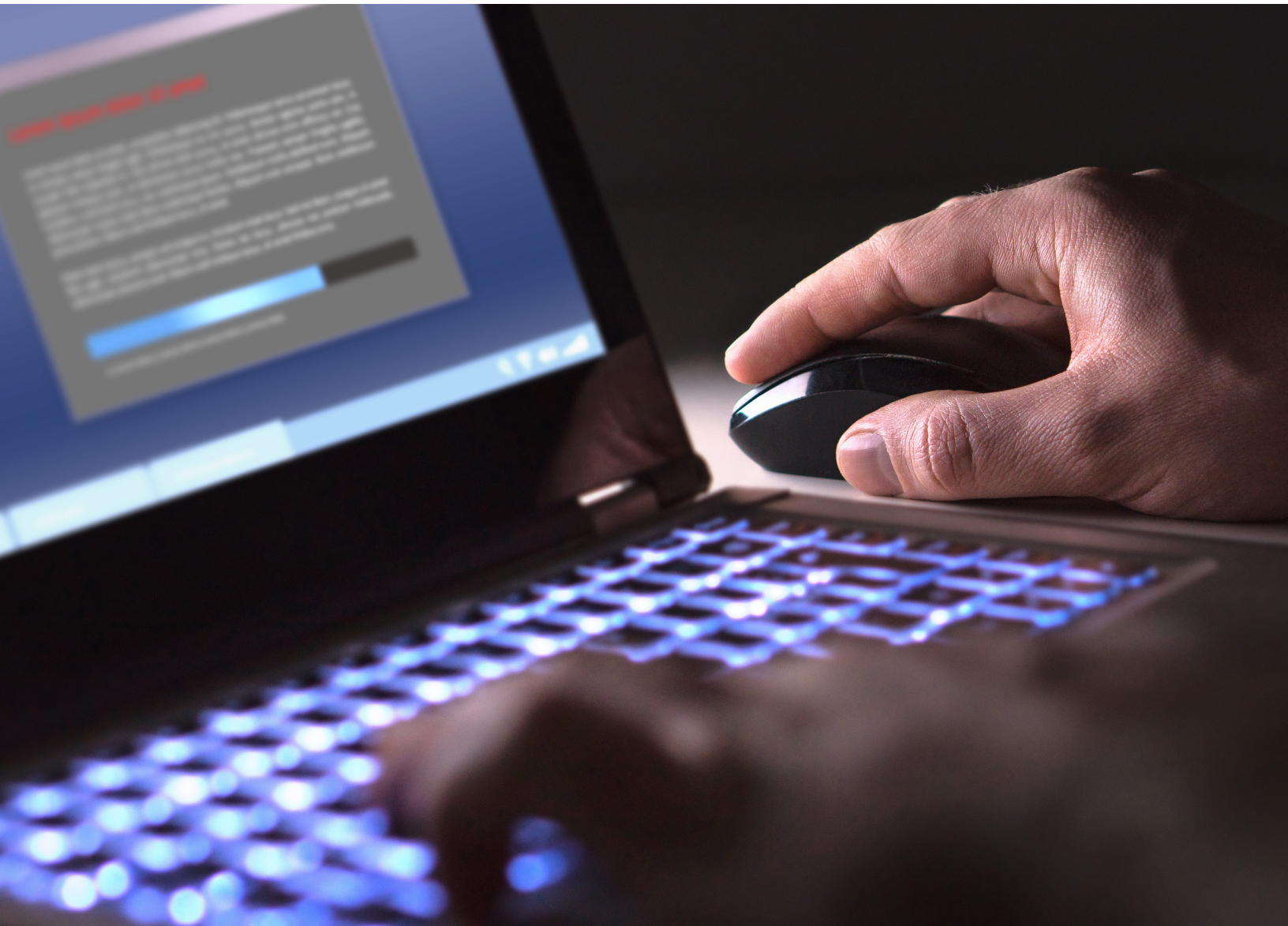
AlixPartners

JUNE 2018

FINANCIALLY DISTRESSED COMPANIES NEED MORE – NOT LESS – FOCUS ON CYBERSECURITY



For executives of under-performing companies, security often takes a back seat, as they devote all their attention to the most important task at hand: averting financial crisis.

They no longer see security measures and precautions as being critical to survival, so they reduce their priority level and cut investments previously allotted to them. As a result, cybersecurity threat exposure increases. In one recent survey, more than half of respondents reported that 26 to 50% of M&A deal target companies experienced data security breaches in the past two years[1].

While funds may be tight, short-changing security can significantly impact recovery. Security breaches will result in additional debts and unanticipated costs. In addition, exploited vulnerabilities will accelerate customer churn, leading to declining revenues. Meanwhile, theft of customer information or confidential business data, such as secrets, patents, and other intellectual property, will decrease asset value in the eyes of potential buyers and may reduce recoveries from which to pay creditors.

CYBER BREACH FACTS AND STATISTICS AT A GLANCE

- Average cost of event: $3.62 million[2]
- Over the past five years, liabilities for a number of data breaches exceeded $100 million
- State, SEC and EU cyber and data protection regulations and fines grow
- Directors hold CEOs accountable for breaches[3]
- Average cost of lost personal record: $141 per record[2]
- Average time to detect incursion: 192 days[2]
- Long-term costs to remediate poor security greatly exceed estimates

1. Donnelley Financial Solutions, Venue Market Spotlight: Cybersecurity, September 30, 2017
2. Ponemon 12th Annual Cost of Data Breach Study, 2017. https://www.ibm.com/security/data-breach
3. NYSE Governance Services and Veracode. Cybersecurity in the Boardroom Survey, 2015. https://www.nyse.com/publicdocs/VERACODE_Survey_Report.pdf

TOP SIGNS OF SECURITY BREACH RISK

- CxOs have lost focus on security and are no longer informed on risks and threats.
- IT is falling behind on routine maintenance and operating with unpatched software.
- Security has let website certificates expire and is following outdated security protocols.
- IT is not compliant with recent requirements in highly-regulated industries (e.g. health and payments).
- Initially, theft of 'crown jewels' goes undetected and incidents unreported in intellectual property (IP)-dependent or highly secure industries (e.g. pharmaceuticals and technology).
- Employees feel disenfranchised and may start to disregard security rules and treatment of IP.
- Turnover of security talent and others with privileged access is high.
- Indications of a security incident are present, but nothing has been publicly communicated.

Companies experiencing financial distress remain accountable for effectively managing security. In December 2017, for example, the Department of Health and Human Services' Office for Civil Rights (OCR) forced the cyber insurance provider of bankrupt 21st Century Oncology to cover security fines for a breach related to HIPAA information that occurred back in 2015[4].

Hidden or undiscovered breaches can also impact company assets even after receivership and selloff. In February 2018, for example, FedEx Corporation discovered that a server inherited from its 2014 acquisition of Bongo International exposed customer driver's license and passport data[5]. This led to negative press for FedEx and unanticipated costs to secure the server and correct the issue.

Guiding a company through a period of financial distress is already a daunting challenge. Taking a pragmatic approach to cybersecurity that rapidly identifies and prioritizes critical vulnerabilities offers a cost-effective mitigation strategy.

1 Identify threat, exposures, and gaps with privacy laws

2 Address critical quick-hit vulnerabilities

3 Resolve unaddressed incidents

4 Take command and communicate with leadership

5 Contain high-value data and strictly control access

6 Maintain security posture

7 Prepare for reinvestment or liquidation of assets

Financially distressed companies don't have to fall prey to hackers. By prioritizing cybersecurity and implementing processes to ensure protection, executives can lower their company's risk.

4. Marianne Kolbasuk McGee. Bankrupt Cancer Clinic Chain's Insurer to Cover Breach Fine, HealthcareInfoSecurity, December 18, 2017. https://www.bankinfosecurity.com/bankrupt-cancer-clinic-chains-insurer-to-cover-breach-fine-a-10536
5. Kim S. Nash and Ezequiel Minaya, Due Diligence Grows at Acquisition Targets in Attempts to Prevent Any Security Surprises, The Wall Street Journal, March 5, 2018, https://www.wsj.com/articles/companies-sharpen-cyber-due-diligence-as-m-a-activity-revs-up-1520226061

AlixPartners

CONTACT THE AUTHORS:

Jon Rigby (jrigby@alixpartners.com), and Gretchen Ruck (gruck@alixpartners.com).

FOR MORE INFORMATION CONTACT:

David Head
Managing Director
+1 248 262 8453
dhead@alixpartners.com

ABOUT US

For nearly forty years, AlixPartners has helped businesses around the world respond quickly and decisively to their most critical challenges – circumstances as diverse as urgent performance improvement, accelerated transformation, complex restructuring and risk mitigation.

These are the moments when everything is on the line – a sudden shift in the market, an unexpected performance decline, a time-sensitive deal, a fork-in-the-road decision. But it's not what we do that makes a difference, it's how we do it.

Tackling situations when time is of the essence is part of our DNA – so we adopt an action-oriented approach at all times. We work in small, highly qualified teams with specific industry and functional expertise, and we operate at pace, moving quickly from analysis to implementation. We stand shoulder to shoulder with our clients until the job is done, and only measure our success in terms of the results we deliver.

Our approach enables us to help our clients confront and overcome truly future-defining challenges. We partner with you to make the right decisions and take the right actions. And we are right by your side. When it really matters.