Press Release

Beazley sees new phishing threats emerge

New York, April 25, 2017

Beazley, a pioneer in cyber and data breach response insurance, today released its Beazley Breach Insights – April 2017 findings based on its response to client data breaches in the first three months of 2017. The specialized Beazley Breach Response (BBR) Services unit observed phishing scams aimed at accessing direct deposit funds emerge as a growing danger in the first quarter of 2017, particularly in the higher education sector. Phishing scams aimed at accessing employee W-2 tax information were also a continuing threat, representing 9% of all breaches handled by Beazley in the first three months of 2017.

During the first quarter of 2017, Beazley's BBR Services division managed 641 data breaches on behalf of clients, compared to 462 breaches during the same period last year. Analysis of breaches handled by Beazley in 2017 to date revealed:

- **Direct deposit deception**
  Beazley has seen an increase in hackers using phishing techniques to infiltrate employee email accounts and change their direct deposit account details. Once hackers have access to an employee's email, they request a password reset from the organization's payroll provider and change the employee's inbox forwarding rule to send all emails from the payroll provider to the target's junk mail. The hackers then change the employee's direct deposit bank account details to their own to steal funds. In addition, they may also access the employee's W2 information and file a fraudulent tax return.

  The majority of direct deposit phishing attempts occurred in the higher education sector where hacks and malware caused 48% of data breaches in Q1 2017, similar to the 50% of breaches they caused in Q1 2016.

- **Ransomware keeps increasing**
  Ransomware attacks continue to proliferate across industries and were 35% higher in Q1 2017 than in Q1 2016. Although the number of ransomware attacks continues to increase rapidly, Beazley's IT service provider partners were able to retrieve seized client data without the client making ransom payments in the majority of incidents.

- **Hospitals hit by unintended disclosure**
  Unintended disclosure – misdirected faxes and emails or the improper release of discharge papers – continued to represent the largest single cause of healthcare losses, leading to 45% of industry breaches in Q1 2017 compared to 46% in Q1 2016. Malicious insiders also persist as a threat in the healthcare industry, accounting for 12% of breaches in Q1 2017, up slightly from 10% in Q1 2016.

- **Financial institutions are still vulnerable**
  Hacks and malware continued to drive the largest proportion of financial institution data breaches, representing 39% of breaches in Q1 2017, equal to the proportion of these breaches in the industry in Q1 2016. Unintended disclosure - sending bank account details or personal information to the incorrect recipient - is another leading cause of data breaches in this industry, representing 31% of breaches in Q1 2017, up from 26% in Q1 2016.

Beazley Group

1270 Avenue of the Americas
Suite 1200
New York, NY 10020
USA

Phone (646) 943 5900
Fax (646) 378 4039

info@beazley.com
www.beazley.com

Press Release

The Beazley BBR Services team offers clients cyber extortion and ransomware response assistance, connecting clients with forensic services to determine if personally identifiable information or protected health information was compromised in the event of a ransomware attack. BBR Services also liaises with service providers on the client's behalf to assist with data decryption, data restoration, or securing bitcoin if an organization decides to pay the ransom.

Katherine Keefe, global head of BBR Services, said: "Organizations continue to face increasingly sophisticated threats as hackers adapt and employ new methods to seize data and funds. Beazley's experienced team works with our insured companies to quickly address reported data incidents, minimize disruption and swiftly put incident investigation and response into action."

Read the Beazley Breach Insights - April 2017 report.

About Beazley Breach Response (BBR)

Beazley has helped clients handle more than 5,000 data breaches since the launch of Beazley Breach Response in 2009 and is the only insurer with a dedicated in-house team focusing exclusively on helping clients handle data breaches. Beazley's BBR Services team coordinates the expert forensic, legal, notification and credit monitoring services that clients need to satisfy all legal requirements and maintain customer confidence. In addition to coordinating data breach response, BBR Services maintains and develops Beazley's suite of risk management services, designed to minimize the risk of a data breach occurring.

Beazley Group

1270 Avenue of the Americas
Suite 1200
New York, NY 10020
USA

Phone (646) 943 5900
Fax (646) 378 4039

info@beazley.com
www.beazley.com

For further information, please contact:

Beazley Group
Hunter Hoffmann
hunter.hoffmann@beazley.com
+1 (917) 344 3329

BZPR_4_25_2017

Note to editors:

Beazley plc (BEZ) is the parent company of specialist insurance businesses with operations in Europe, the US, Canada, Latin America, Asia, the Middle East and Australia. Beazley manages six Lloyd's syndicates and, in 2016, underwrote gross premiums worldwide of $2,195.6 million. All Lloyd's syndicates are rated A by A.M. Best.

Beazley's underwriters in the United States focus on writing a range of specialist insurance products. In the admitted market, coverage is provided by Beazley Insurance Company, Inc., an A.M. Best A rated carrier licensed in all 50 states. In the surplus lines market, coverage is provided by the Beazley syndicates at Lloyd's.

Beazley is a market leader in many of its chosen lines, which include professional indemnity, property, marine, reinsurance, accident and life, and political risks and contingency business.

For more information please go to: www.beazley.com