LESSONS LEARNED

Déjà vu all over again

1.1 Million Users impacted in CareFirst BlueCross BlueShield Information Security Breach

In May, CareFirst BlueCross BlueShield (CareFirst) announced it had been subjected to a sophisticated information security cyberattack, exposing information on approximately 1.1 million current and former CareFirst members. According to an outside cybersecurity firm's investigation, the breach occurred in June 2014 and gave hackers access to user names, dates of birth, email addresses and subscriber identification numbers.

This is the third Blue Cross or Blue Shield Company (BCBS) to recently announce it has been hacked. BSI issued "Lessons Learned" reports on two other BCBS plans that reported cyber-attacks earlier this year: Anthem Inc., which impacted around 78.8 million individuals, and Premera Blue Cross with 11 million affected by its hacking incident.

According to CareFirst, the company was first advised of the breach by Mandiant, the cyberforensics unit of security vendor FireEye, as part of CareFirst's proactive examination of their Information Technology security environment. Mandiant identified evidence of an intrusion and the unauthorized access.

bsi.

...making excellence a habit.™

HealthcareInfoSecurity quoted Mandiant's managing director Charles Carmakal as saying, "The intrusion was orchestrated by a sophisticated threat actor that we have seen specifically target the healthcare industry over the past year." According to CareFirst, "the attackers gained limited, unauthorized access to a single CareFirst database." (McGee, 2015)

The attackers could have acquired user names which would have been created to access the company's website, according to CareFirst. However, "user names must be used in conjunction with a member-created password to gain access to underlying member data." The company indicated that passwords are fully encrypted and stored in a separate system. The database that was breached "contained no member Social Security numbers, medical claims, employment, credit card or financial information." (CareFirst)

Using CareFirst information and quotes from the story in HealthcareInfoSecurity, a review of the facts of the case indicate how this incident may have been avoided or its impact minimized if a verifiable management system standard, such as ISO/IEC 27001 for an Information Security Management System (ISMS), had been in place.

According to the CareFirst website, the cyberattack was "discovered as a part of the company's ongoing Information Technology (IT) security efforts ..."

Under A.9 Access control, ISO/IEC 27001:2013 recommends a full evaluation and implementation of controls covering:

- Business requirements of access control (A.9.1)
- User access management (A.9.2)
- User responsibilities (A.9.3), and
- System and application access control (A.9.4)

Also to ensure there is more of a real-time analysis and detection process,

A.12.4.1 Event logging would be in order

Control

Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

A.12.6.1 Management of technical vulnerabilities

Control

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

HealthcareInfoSecurity reports, "Mandiant's managing director Charles Carmakal said, "The intrusion was orchestrated by a sophisticated threat actor that we have seen specifically target the healthcare industry over the past year...".

ISO/IEC 27001:2013

A.6.1.4 Contact with special interest groups

Control

Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

Note: Information sharing is critical when an entire industry has been targeted to mitigate the risk of it occurring as there is a higher level of preparation and awareness. This would then feed into the Risk Planning and Operations process (6.1 Actions to address risks and opportunities and 8.2 Information security risk assessment and 8.3 Information security risk treatment.)

bsi.

CareFirst noted on their website the breach "was discovered as a part of the company's ongoing Information Technology (IT) security efforts in the wake of recent cyberattacks on health insurers. CareFirst engaged Mandiant – one of the world's leading cybersecurity firms – to conduct an end-to-end examination of its IT environment. This review included multiple, comprehensive scans of the CareFirst's IT systems for any evidence of a cyberattack.... Mandiant completed its review and found no indication of any other prior or subsequent attack or evidence that other personal information was accessed."

ISO/IEC 27001:2013

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system; and

b) the requirements of these interested parties relevant to information security.

Note: Being proactive is excellent, but using technology-only solutions to monitor and evaluate a system is not effective. An organization must understand the entire context of its business environment. Only then can the proper safeguards and approach be implemented. Analyses of the root causes involved in other recent security breaches such as this show that efforts to protect an organization using solutions based solely on technology do not achieve the organization's objectives of cybersecurity, nor are they viable over the long term. In similar cases, phishing campaigns were used to obtain security credentials. In those cases, technology was of little use. Security must be addressed from a more holistic approach of people, process and technology. BSI has developed a whitepaper on this subject, ***People, Process, Technology - The three key elements for a successful information security system***, which can be found on our website.

Bibliography

CareFirst. (n.d.). CareFirst BlueCross BlueShield has been the target of a cyberattack. Retrieved from http://www.carefirstanswers.com/

McGee, M. K. (2015, May). CareFirst BlueCross BlueShield Hacked. Retrieved from http://www.healthcareinfosecurity.com/carefirst-bluecross-blueshield-hacked-a-8248?rf=2015-05-21-eh&mkt_tok=3RkMMJWWfF9wsRons6XNZKXonjHpfsX57ewtWqSg38431UFwdcjKPmjr1YIHRcJ0aPyQAgobGp5I5FEIT7HYRrhpt6cOXA%3D%3D

bsi.

For information on Lessons Learned regarding other cybersecurity breaches, visit our website on www.bsigroup.com/en-us

BSI Group America Inc.
12950 Worldgate Drive, Suite 800
Herndon, VA 20170
USA

Tel: 1 800 862 4977
Fax: 1 703 437 9001
Email: inquiry.msamericas@bsigroup.com
Web: www.bsigroup.com/en-us

BSI Group Canada Inc.
6205B Airport Road, Suite 414
Mississauga, Ontario
L4V 1E3
Canada

Tel: 1 800 862 6752
Fax: 1 416 620 9911
Email: Inquiry.canada@bsigroup.com
Web: www.bsigroup.ca
www.bsigroup.ca/fr

BSI/USA/456/MS/715/E