Heartbleed vulnerability

An urgent internet security wake up call

What is 'Heartbleed' and how does it impact you?

'Heartbleed' is a security vulnerability found in many (66%) of the web servers in use today. It allowed attackers to steal confidential information or private encryption key(s) from your website without leaving a trail.

Exposed data may include usernames and passwords, credit card details, intellectual property, personal information of your users, customers and systems.

This may have widespread implications including immediate and ongoing financial, legal, regulatory and reputation consequences for you, your customers and your supply chain.

What is your technical exposure?

Technically, 'Heartbleed' is a vulnerability in OpenSSL cryptographic software. More notable software using OpenSSL are open- source web servers like Apache and Nginx. If your organisation uses an OpenSSL version that is earlier than 1.0.1g, it is likely that your system is vulnerable to 'Heartbleed'.

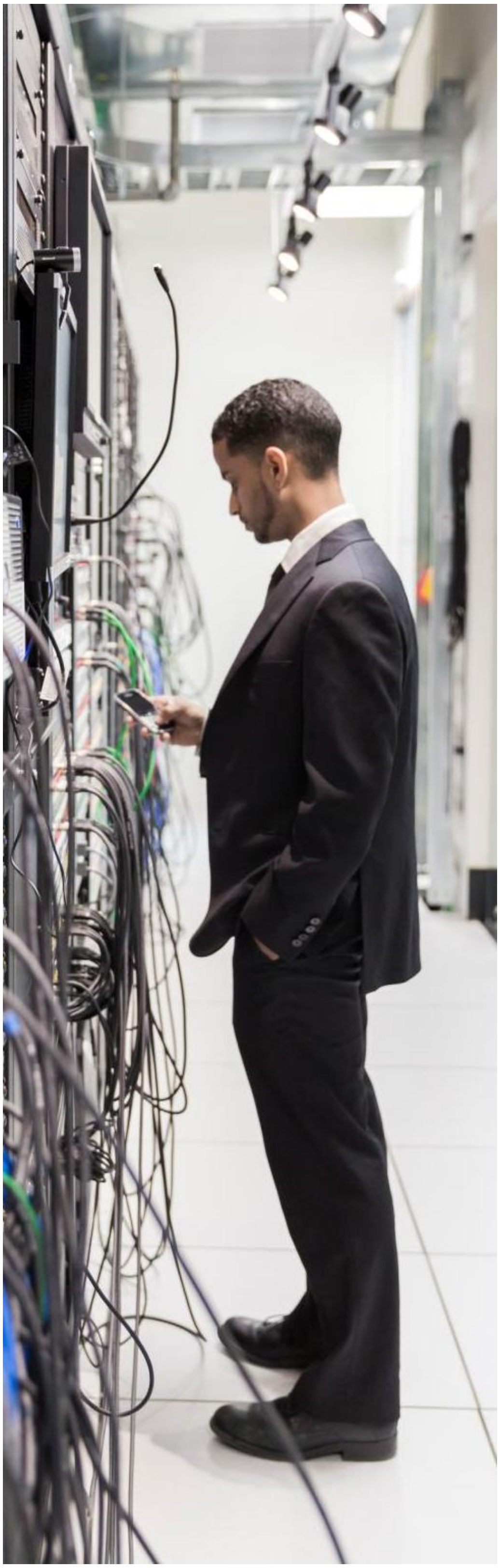
As 'Heartbleed' leaves very little forensic evidence, it is extremely difficult to know if any information has been compromised.

More worryingly, it was also revealed that the 'Heartbleed' vulnerability has been in existence for two years but was only discovered in April 2014.

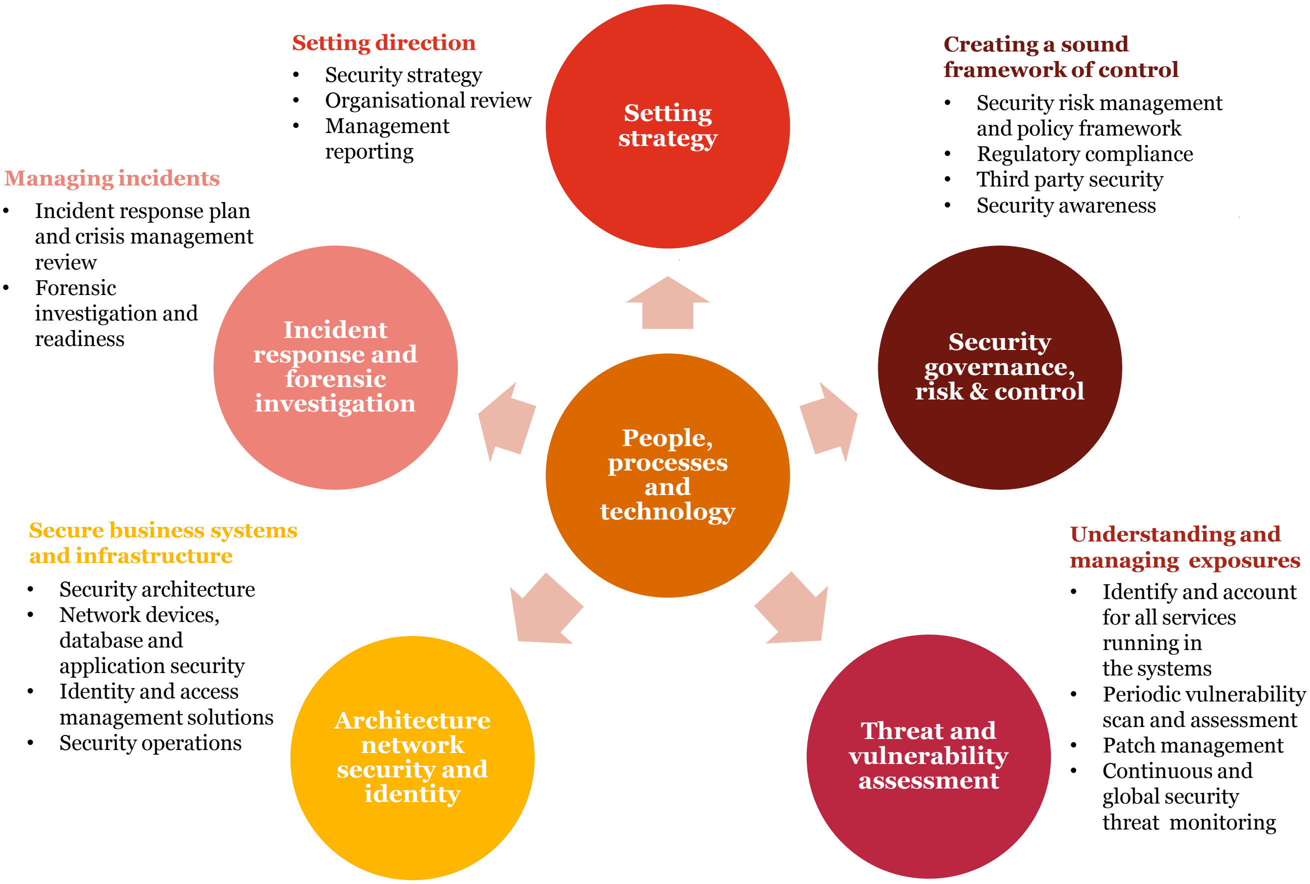
What precautionary measures can you take?

While there are patches currently available to fix 'Heartbleed', you should also ensure that you conduct a comprehensive scan of your systems and that all vulnerabilities are fixed as soon as possible. Following that, you should inform all users to change their log-in passwords and remind them to do so periodically.

In the long run, we believe that incorporating sound vulnerability management into your overall IT security framework will help your organisation assess and manage future security vulnerabilities.



Security framework for robust vulnerability management



People, processes and technology

Setting strategy

Setting direction

- Security strategy
- Organisational review
- Management reporting

Security governance, risk & control

Creating a sound framework of control

- Security risk management and policy framework
- Regulatory compliance
- Third party security
- Security awareness

Threat and vulnerability assessment

Understanding and managing exposures

- Identify and account for all services running in the systems
- Periodic vulnerability scan and assessment
- Patch management
- Continuous and global security threat monitoring

Architecture network security and identity

Secure business systems and infrastructure

- Security architecture
- Network devices, database and application security
- Identity and access management solutions
- Security operations

Incident response and forensic investigation

Managing incidents

- Incident response plan and crisis management review
- Forensic investigation and readiness

How confident are you in…

- … your vulnerability management plan and is it aligned to your overall security framework?
- … identifying the systems that are vulnerable to 'Heartbleed' and other potential technology risks?
- … managing the cost for remediation?
- … your people's awareness of the systems' vulnerabilities and their responsibilities for the associated risks?
- … your preparedness to handle a security breach?

How we can help you build IT risk resilience

PwC brings you a multi-disciplinary team with established credentials to help you identify IT risks and assist you with designing of an IT governance and risk management framework which enhances your It risk resilience.

In the particular case of 'Heartbleed', we have developed a methodology to assist our clients in identification and suggested remediation. We have the tools to validate whether or not any of your systems are vulnerable or exploitable. More importantly, we can help you look beyond just a one-time vulnerability and help you implement a sound vulnerability management strategy. With our assistance, you can optimise your systems control, giving you better management of risk and improved decision-making.

To have a deeper conversation, please contact:

Tan Shong Ye
Partner
+65 6236 3262
shong.ye.tan@sg.pwc.com

Mark Jansen
Partner
+65 6236 7388
mark.jansen@sg.pwc.com

Chan Hiang Tiak
Partner
+65 6236 3338
hiang.tiak.chan@sg.pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.