THALES

New Technologies and Old Habits Driving Data Breaches and Risk in Global Healthcare

Majority of global healthcare enterprises using cloud, big data and IoT without securing sensitive data

Thales, a leader in critical information systems, cybersecurity and data security, announces the results of its 2017 Thales Data Threat Report, Healthcare Edition, issued in conjunction with analyst firm 451 Research. The fifth annual report indicates global healthcare IT professionals are confronting a rapidly changing, challenging landscape, with 66% of respondents experiencing a data breach and 88% feeling vulnerable as a result. In response, 73% are increasing IT security spending to offset threats to data.

Click to Tweet: New tech, old habits leading to sensitive healthcare data risks #2017DataThreat http://bit.ly/2kua9Ud

Out with the Old, In with the New?

While healthcare records have always been a desirable commodity on the black market, technological changes have further complicated its storage and protection. Despite the risks that come from increased access points, 65% of global healthcare respondents report their organizations are deploying to cloud, big data, and IoT environments without adequate data security controls. The global healthcare industry is also adopting some of these technologies for sensitive data use wholesale, with 51% of global healthcare respondents deploying sensitive data to SaaS and IaaS environments, 36% to big data environments and 34% to IoT environments.

Despite the changing face of healthcare data deployments, many organizations remain stubbornly focused on network and endpoint security. Fifty-three percent of global healthcare respondents are spending the most on network security, followed by endpoint security at 51%. Additionally, 67% of global healthcare respondents perceive network security as highly effective at stopping data breaches, followed closely by endpoint security (66%). While network and endpoint technologies are a required element of an organization's IT security stance, they are increasingly less effective at keeping external attacks at bay, and in securing cloud, big data, IoT and container deployments – which result in data being distributed, processed and stored outside corporate network boundaries.

Perceived Data Protection Barriers – and Threats

In response to questions about why they are not implementing more effective data security controls, 43% of global healthcare respondents cited 'lack of staff', followed by 'perception of complexity' (37%) and 'lack of organizational buy-in' (also 37%). Further exacerbating these barriers are internal and external threats. At 63%, privileged users top the list of internal threats. Executives are second at 51%, followed by external service providers with internal account access (29%). When it comes to external threats, cyber-criminals are considered the greatest challenge by 47%, with hactivists a distant second (16%) and competitors in third (13%).

Encryption Playing Larger Role in Healthcare Data Protection

Across the board, encryption is the technology of choice when it comes to protecting sensitive data residing within cloud, IoT and container environments. Fifty-eight percent of global healthcare respondents opt to encrypt data in the public cloud, with the survey yielding similar numbers for IoT data (58%) and container data (60%). Data sovereignty, a hot topic in light of concerns about new privacy regulations and government snooping, is also spurring encryption adoption. The technology is

the clear choice for satisfying local data privacy laws such as the EU's General Data Protection Regulation (GDPR) by 66% of global healthcare respondents. Also notable are the 33% searching for local data locations or cloud providers to meet data residency needs.

Peter Galvin, VP of strategy, Thales e-Security says:
"Globally, healthcare companies are under pressure. The use of advanced technologies is increasingly impacting security decision-making, as our data privacy and residency requirements. For healthcare data to remain safe from cyber exploitation, security strategies need to move beyond laptops and desktops to encompass an 'encrypt everything' approach that best suits a world of internet-connected heart-rate monitors, implantable defibrillators and insulin pumps. Adhering to the security status quo will create vulnerabilities that lead to breaches, and further erode customer trust."

Healthcare organizations interested in improving their overall security postures should strongly consider:

- Deploying security tool sets that offer services-based deployments, platforms and automation
- Discovering and classifying the location of sensitive data, particularly within IoT and container environments
- Leveraging encryption and "Bring Your Own Key" (BYOK) technologies for the cloud and other advanced environments

Please download a copy of the new 2017 Thales Healthcare Data Threat Report for more detailed security best practices.

Visit Thales at booth #7082, HIMSS Conference, Orlando, Florida, February 19-23, 2017.
For industry insight and views on the latest key management trends check out our blog www.thales-esecurity.com/blogs.

Follow Thales e-Security on Twitter @Thalesesecurity, LinkedIn, Facebook and YouTube.

Contact:

Dorothée Bonneil
Thales Media Relations – Security
+33 (0)1 57 77 90 89
dorothee.bonneil@thalesgroup.com

Liz Harris
Thales e-Security Media Relations
+44 (0)1223 723612
liz.harris@thales-esecurity.com