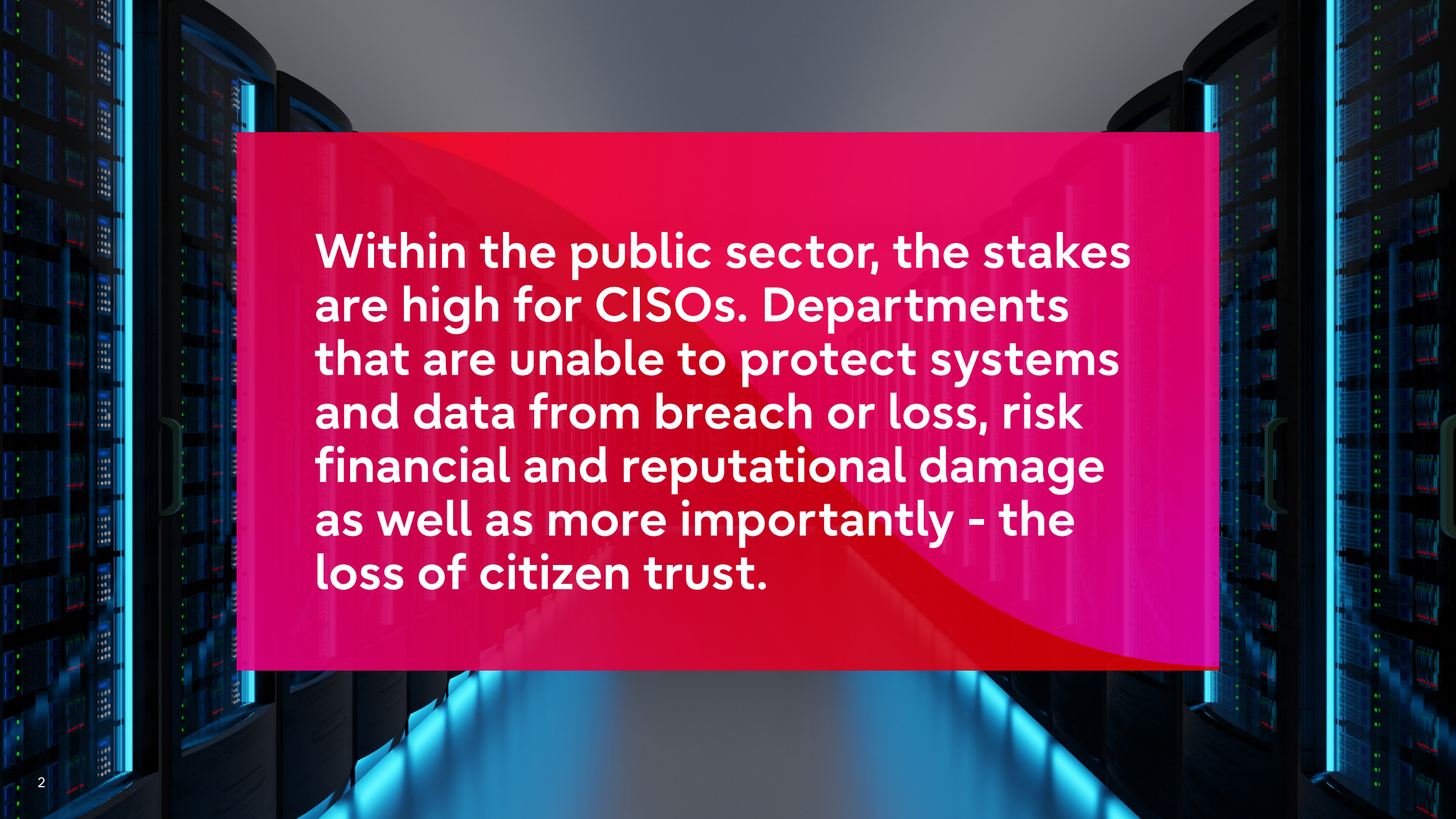
FUJITSU

With cyber threats on the rise – are public sector entities doing enough to keep citizen data safe from loss and attack?



Within the public sector, the stakes are high for CISOs. Departments that are unable to protect systems and data from breach or loss, risk financial and reputational damage as well as more importantly - the loss of citizen trust.

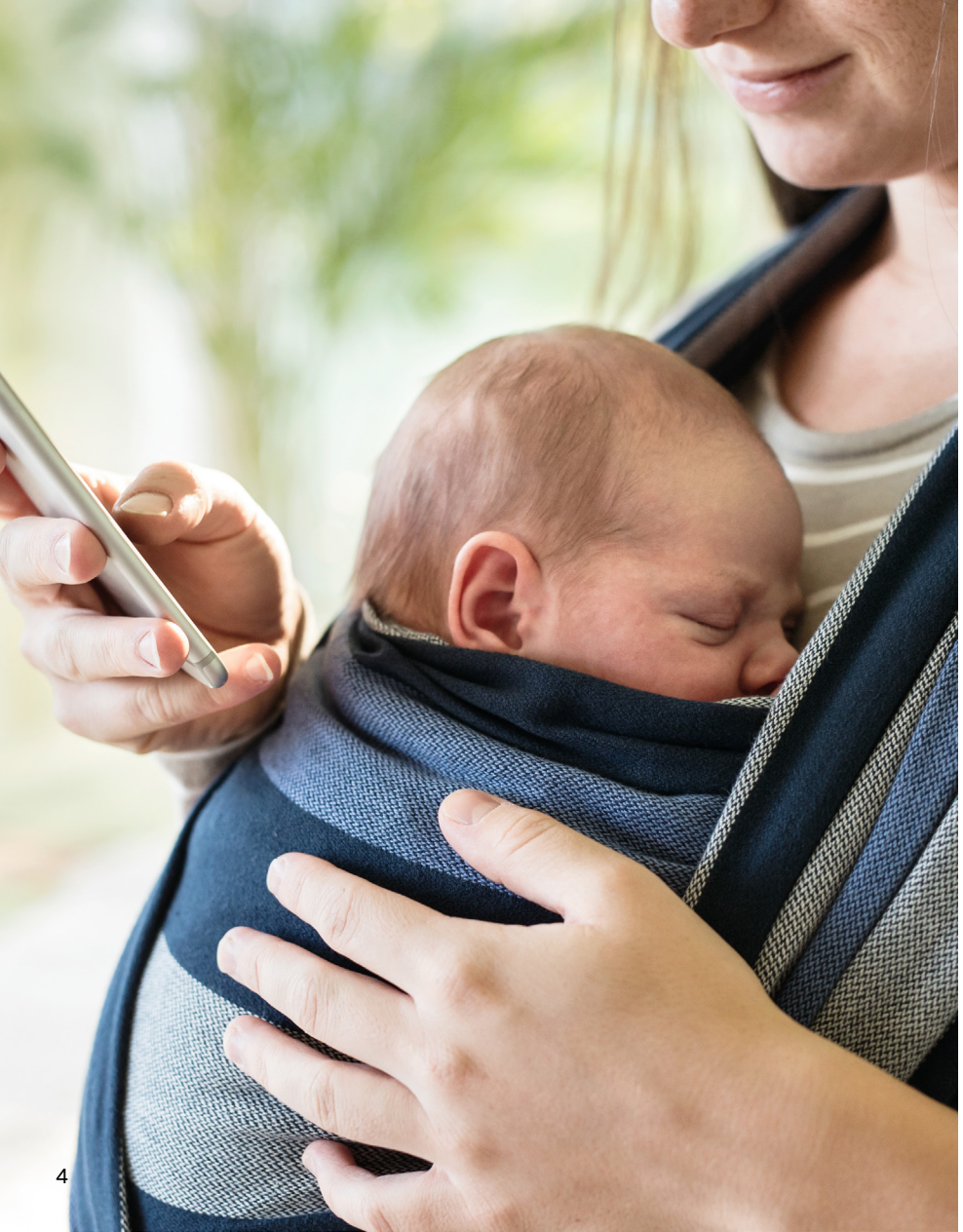
Government services provide security, societal order, and economic stability.

However, with a significant increase in cyber-attacks and threats – 304 million global attacks in 2020 increased by 148% to 753 million in 2021 – governments have a significant challenge on their hands to keep citizen data and systems safe and secure. If you factor in what's now happening with Russia and the Ukraine, 2022 cyber-attacks could well reach over 1 billion in number.

While ransomware in government is devastating, potentially resulting in the loss of 30+ years of data, it's important to realize building a cyber-resilient public sector is not just about external threats. This came clearly into focus in 2021 with the deletion of around 22 terabytes of Dallas PD data – 7 terabytes of which could not be recovered – seriously impacting police cases and citizen trust. While later investigation revealed the deletion was accidental and due to poor training and recklessness rather than malicious intent, the fact it happened exposed the need for improved IT and cyber security expertise in handling and migrating data within government and the public sector.

In the Dallas PD example, the IT worker failed to verify the existence of copies, paid little attention to backups before deleting the data, and had no technological solution to monitor sensitive data sessions to prevent catastrophic mistakes. This could have been avoided through better training and leveraging appropriate procedures, processes, and tools.

However, within the public sector, ensuring the correct processes and procedures are in place for different environments can be challenging. Public sector entities are often still working on decades-old legacy systems and technology has changed so much in this time. When migrating from mainframe technology to client-server technology in existing data centers and to the Cloud, each requires the correct toolset, and this is easily where issues can occur. According to Gartner, over 90% of breaches can be attributed to client misconfiguration. Tools are out there and available to prevent these attacks - however, they need to be correctly configured and implemented for each environment.



Cyber security is not just a governmental issue

Today, we are talking about a vast array of digital public sector records such as healthcare, crime, tax, education, property, birth, and death. So much personal data is now collected and stored by the government on the average US citizen – where they live, who owns the property they live in, how they paid their taxes etc. that any cyber-attack, ransomware attack, and data loss is considered a catastrophic failure of trust.

The impact on citizens can be both direct and indirect. Going back to the Dallas PD data deletion example, how much better would it have been to have the correct procedures and safeguards in place to ensure this catastrophe never happened? With data lost and no backups to turn to, the question is how many criminal cases will now have to be dropped? How many individuals will now not get the justice they deserve? Consider a data breach at a city, state, or federal level - imagine the disruption and destabilizing societal effect of a breach that's linked to voting and election results. What could be the aftermath for citizens of such an event?

Prevention is better than cure

Where cyber security is concerned, understanding the challenges and ensuring proper processes and tools are in place is the key to effective protection. However, many organizations don't have the necessary expertise and skills to do this internally, a fact supported by Gartner, which estimates that by 2025 at least 50% of cyber security will be outsourced to managed service providers.

Cyber security is a constantly evolving area, with new attack surfaces and new actors constantly coming into play trying to penetrate government departments and agencies. It's far more efficient and cost-effective to have the expertise, tools, and processes in place ahead of time as opposed to dealing with the aftermath and fallout of an incident.

Today, threats are going to happen, and at Fujitsu, we believe prevention is better than cure. With decades of global security expertise, we bring to bear the best practices and proper toolsets to proactively detect and prevent attacks. Within our organization, we're not just looking at individual customers, we're looking at dashboards that see events taking place around the world. We incorporate best practices and take what we learn at both a global and more local level, to enhance our cyber security service offering for the benefit of all our customers. This means when a government department or public sector entity comes to us and asks for the implementation of the correct monitoring solution, we can help. If they want incident detection, investigation, and backup and recovery in place, we can help. If they want to cut threat detection and response times, we can help.

FUJITSU

Contact us at Fujitsu to discuss the ever-evolving cyber security landscape. Discover how we are helping public sector entities to keep their citizen data safe from loss and attack.

For more information check the Public Sector webpage.

Author:

Matthew Hon
CTO Public Sector Fujitsu North America

Matthew is responsible for helping government agencies leverage technology solutions to address business and society problems.