

FIGHTING AGAINST CYBER HACKS AND SECURITY BREACHES

PUBLISHED
31 May 2018

CATEGORY
Other

OTHER · MAY 2018

Fighting Against Cyber Hacks and Security Breaches

Anyone that has so much as glanced at the news headlines over the last two years is aware that cybersecurity and the prevention and mitigation of harm caused by cyberattacks is a major concern for both industry and the government, and with continued concerns about election integrity and external influence campaigns on elections, the government's interest in enhancing cybersecurity will only continue. Compounding this concern is the continued growth in smart infrastructure that is internet enabled (e.g., the number of devices connected to the internet via sensors and the push for a smart electrical grid).

The Department of Homeland Security (DHS), in its capacity as the chief coordinator of internal security initiatives – whereas other agencies tend to handle security initiatives that are primarily external (for example, the State and Defense Departments) – announced the creation of the National Risk Management Center (NRMC). Kirstjen Nielsen, the Secretary for Homeland Security, created the NRMC so that it can concentrate on evaluating and mitigating threats against critical, internal infrastructure. Initially, the center will focus on energy, finance, and telecommunications and conducts sprints throughout 2018 to quickly build up the center's ability to meet its mission.

It is hoped that the new center will be the focal point of cybersecurity protection within the federal government according to Secretary Nielsen, and the Executive Branch has immediately begun work with both the House of Representatives and the Senate to enshrine the center and the organizational changes it entails into law. While the House already passed a bill, Senators Hassan and Portman introduced the DHS Cyber Incident Response Teams Act of 2018 to establish the Center's framework and to allow DHS to better coordinate with other federal agencies and private organizations. The center endeavors to also establish itself as a sort-of 911 for regional branches of government to allow them to call-in federal resources if a crisis were to occur.

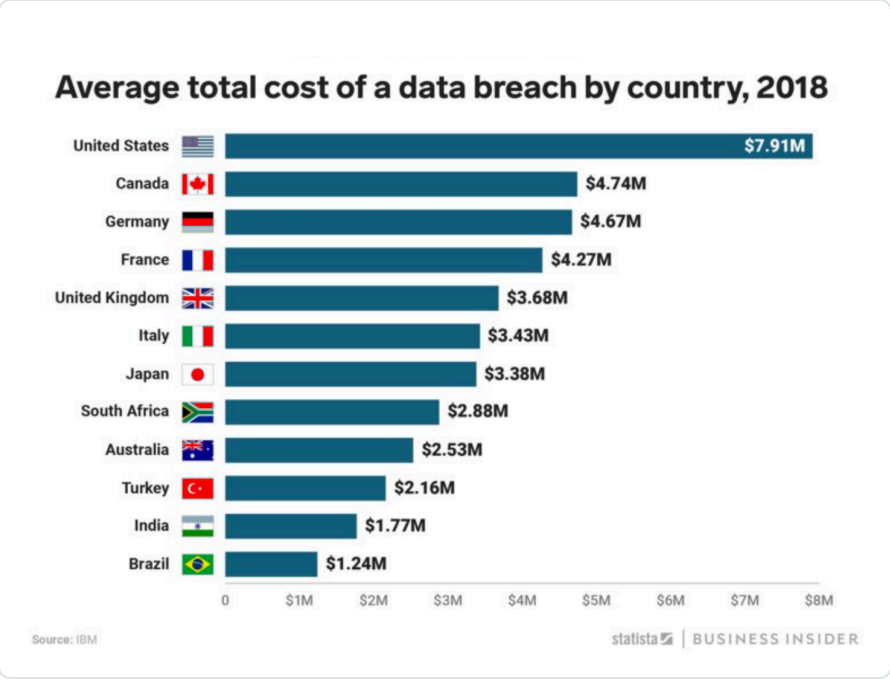
The establishment – and possible enshrinement in law – of the center could not come at a more suitable time. According to a recent report by SecurityScoreCard - a New York Firm that has developed a common framework for companies to communicate about and evaluate security – state and local governments – while having taken action to help bolster their security posture – are still, nonetheless, in a relatively vulnerable position. In a recent report, it rated four states, two counties, and a city on their overall security, endpoint protection, IP reputation efforts, network security, and patching processes.

Notably, the best overall scores – using an A-F scale – were only Cs, and there was only one A (New Hampshire's Endpoint Security). What is likely highly concerning for security experts – especially given the cause of the Experian attack – is that every unit of government except for one received an F for patching. It is evident from this report – which didn't even begin to address some internal threats that could be caused by poor access controls for example – is that additional effort, best practices development, and implementation resources are

© 2018 ThreatRate Risk Management. All Rights Reserved

needed for local governments; efforts such as DHS's NRMC may provide such resources to move the mark on cybersecurity at the local governmental level.

The United States is not alone in needing significant improvement in its cybersecurity posture. Japan has recently introduced new efforts to bolster its cybersecurity efforts both in government and industry – where it has lacked relative to peer countries. Their efforts involve working to better incorporate cybersecurity governance into corporate structures – especially at the C-suite level – and to encourage more investment in cybersecurity. In addition to government coordination efforts, the Japanese government is offering tax credits to help incentivize governments to improve their cybersecurity efforts. Globally, governments will likely have to continue such efforts if there is going to be noticeable improvements in mitigating cybersecurity threats and mitigating the harm caused by inevitable cyberattacks.



Soundbite analytics

- By 2019, costs associated with data breaches is expected to surpass $2 trillion dollars.
- The average data breach cost is expected to be more than $4 million.
- In almost 60% of incidents, the governments take more than a year to discover the breach.
- Only 55% of Japanese companies perform Security Risk Assessments (SRAs).
- Only 27% of Japanese companies have a Chief Information Security Officer (CISO).

© 2018 ThreatRate Risk Management. All Rights Reserved

SOURCES

1 https://www.wired.com/story/dhs-national-risk-management-center/

2 https://securityscorecard.com/company

3 https://explore.securityscorecard.com/rs/797-BFK-857/images/2018%20Government%20Cybersecurity%20Report.pdf

© 2018 ThreatRate Risk Management. All Rights Reserved



Risk intelligence that keeps you safe

ABOUT THREATRATE

ThreatRate helps you benchmark your risk management strategy against rapidly evolving global and local trends, with real-time, actionable analytics and insights.

For more information contact us at

info@threatrate.com

MEMBERS HAVE ACCESS TO

100+
risk-focused reports published annually

API
customised access option

Dashboards
customised dashboards and infographics

Experts
ThreatRate analysts with cross-industry depth

© 2018 ThreatRate Risk Management. All Rights Reserved

ThreatRate RISK MANAGEMENT