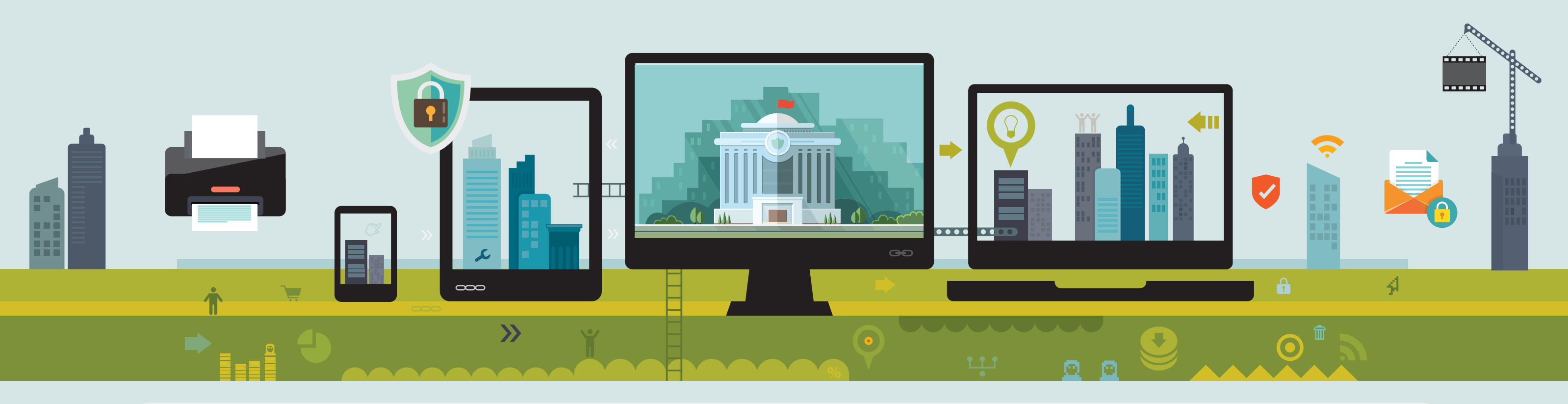
An IDC infographic sponsored by HP Inc.

IT Procurement: The Weak Link in Government Security



IDC evaluated 130 Requests for Proposals (RFPs) from government organizations in nine countries to determine the extent to which device security is being considered in public procurement of PCs and printers. This infographic highlights the results of that study.

Device Security and the Emerging Threat to Governments

A dynamic threat landscape pervades society, making IT systems vulnerable to an ever-increasing and ever-changing set of security attacks.

In recent years, government departments and agencies have drawn attention from threat actors seeking to exfiltrate confidential data, or simply to obstruct and undermine the continuity of nation-states' governance.

2017 — **WannaCry Ransomware Attack**

- 300,000 computer systems in 150 countries affected in five days
- Worms scanned the LAN and WAN networks of connected machines to find and attack other vulnerable hosts
- Over 1/3 of health trusts in the UK National Health Service were disrupted, resulting in 19,000 canceled appointments, including surgeries[1]

2016 — **Attacks on U.S. Government Agencies**

- Over 30,899 cyber incidents experienced compromising information/system functionality
- 16 deemed "major incidents" by the Office of Management and Budget (OMB)[2]

Frequently purchased devices such as PCs and printers are often regarded as commodity items by government departments and agencies.

This exposes agencies to risk if the potential security vulnerabilities of these devices are not consciously considered at the moment of purchase.

[1] *https://www.calyptix.com/top-threats/biggest-cyber-attacks-2017-happened/*

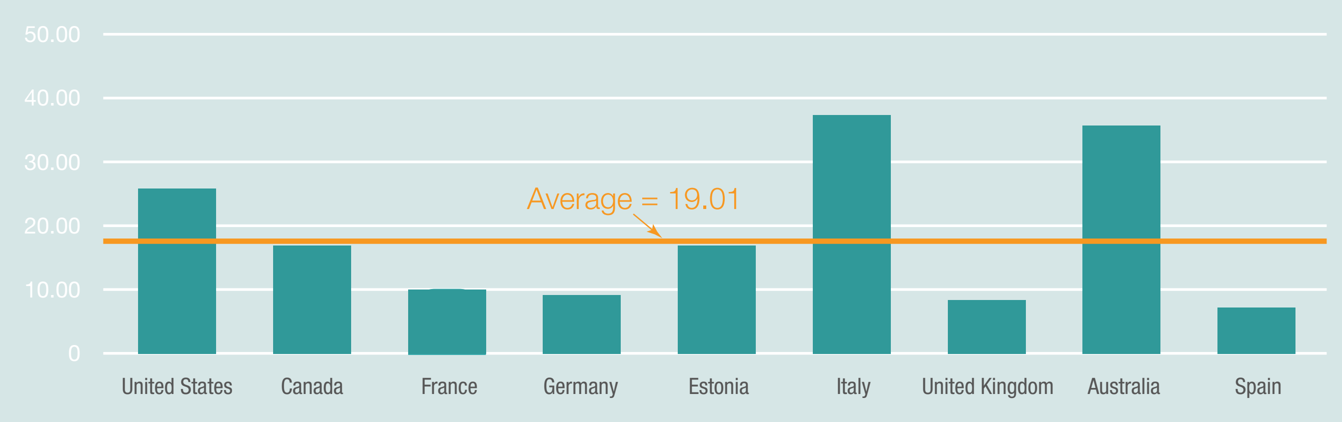
[2] *Office of Management and Budget, "Federal Information Security Modernization Act of 2014, Annual Report to Congress, Fiscal Year 2016," March 10, 2017.*

Countries Can Improve at Specifying Security Requirements

The country scores show a spread between **7.66 and 37.79**, out of a possible 100.

The average index is **19.01**, and the median score is **17.25.**

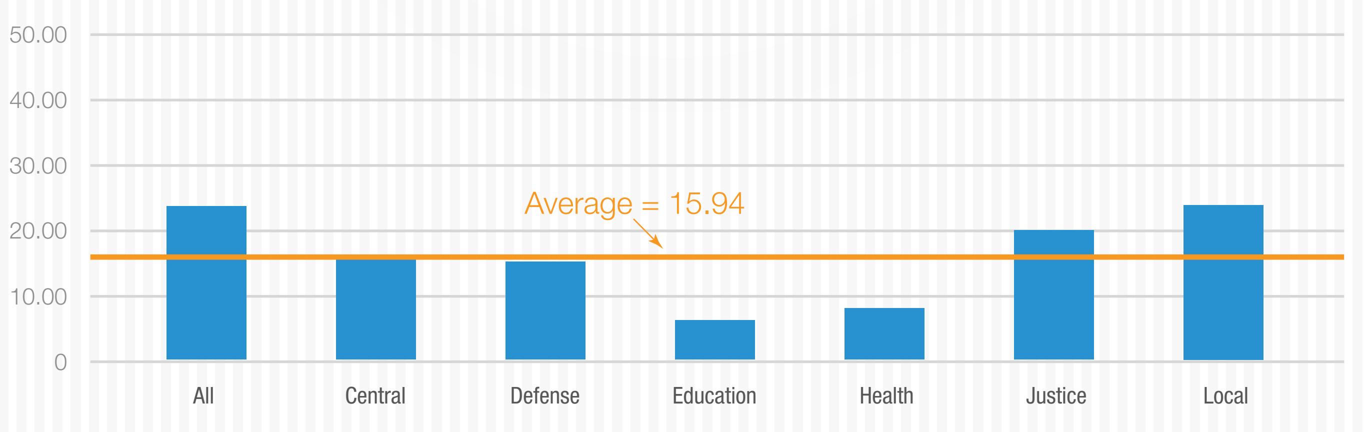
COUNTRY INDEX



Source: IDC's Government Procurement Device Security Study, 2018

Government Sectors with Sensitive Data Exposed

INDEX BY SUBSECTOR FOCUS



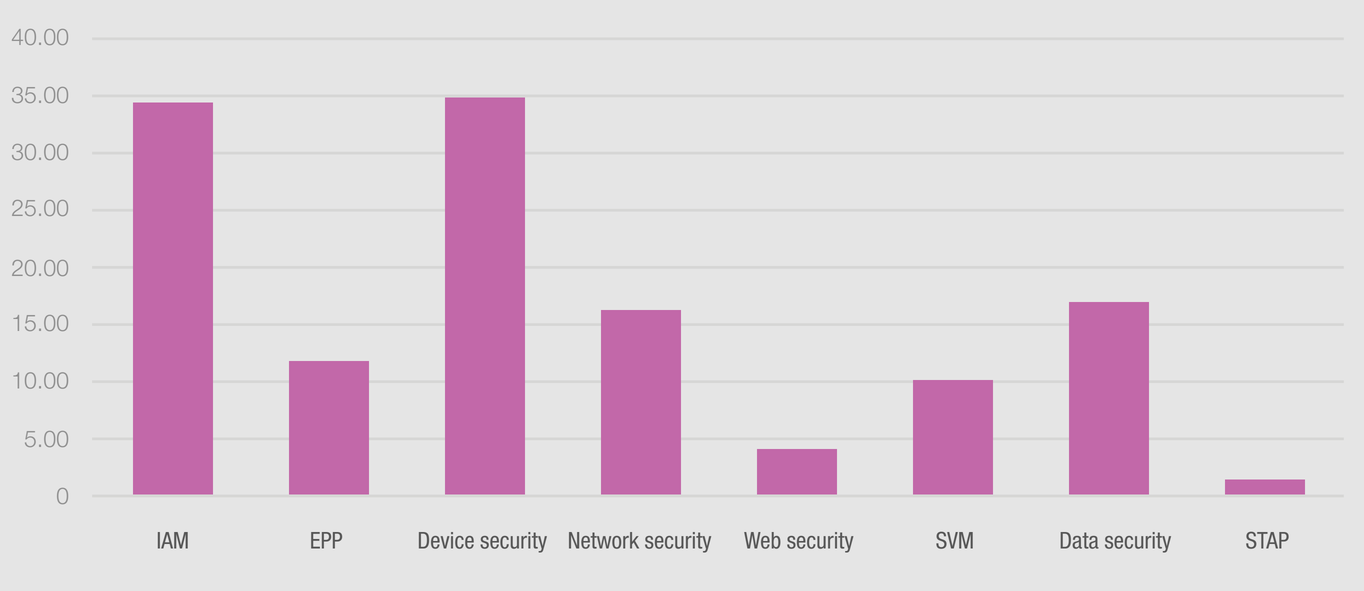
Source: IDC's Government Procurement Device Security Study, 2018

In Education and Health, where sensitive personal data is regularly processed, the scores are low enough to be of primary concern **(6.77 and 7.31 respectively).**

67% of Education RFPs had **no** specified security requirement.

Physical Device Security and IAM: Most-Cited Requirements

SECURITY CATEGORY INDEX



Source: IDC's Government Procurement Device Security Study, 2018

Web security and analytics capability (STAP) are particularly **weak**.

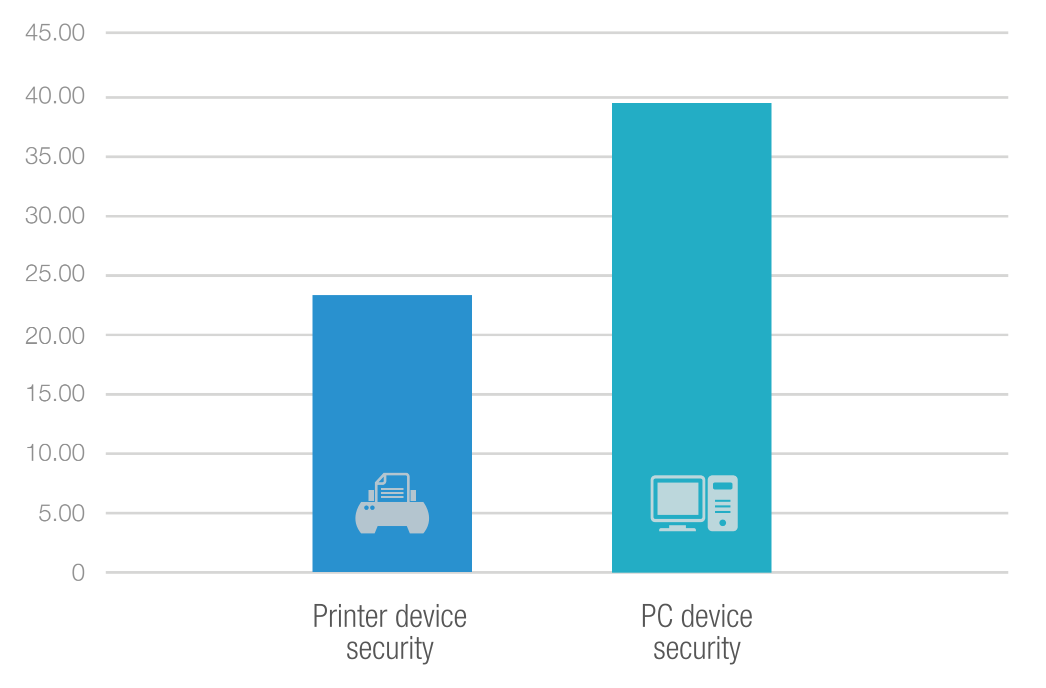
Data security is worryingly low, given the incoming GDPR legislation in Europe.

Device-Based Print Security: Overlooked

Printer RFPs are **72%** less likely to specify security requirements than PC RFPs.

Printer security represents a key area of potential overlooked vulnerability for organizations.

SECURITY CATEGORY INDEX (DEVICE SECURITY ONLY)



Note: Figure shows data for the device security category only; no other security category showed significant differences between PC and printer requirements.

Source: IDC's Government Procurement Device Security Study, 2018

IDC Recommendations for Governments

Modern threats attack devices in ways that traditional software-based solutions cannot detect and protect against.

Consider security as part of the device — not as an afterthought.

All devices are not equal. Look for those with built-in security to defend against modern threats.

For the full story on IDC's Government Procurement Security Index, click here for the white paper, "IDC Government Procurement Device Security Index 2018: Public Sector PC & Printer RFPs Lack Basic Security Consideration," sponsored by HP Inc.

4AA7-3692EEW