AXA

XL Insurance

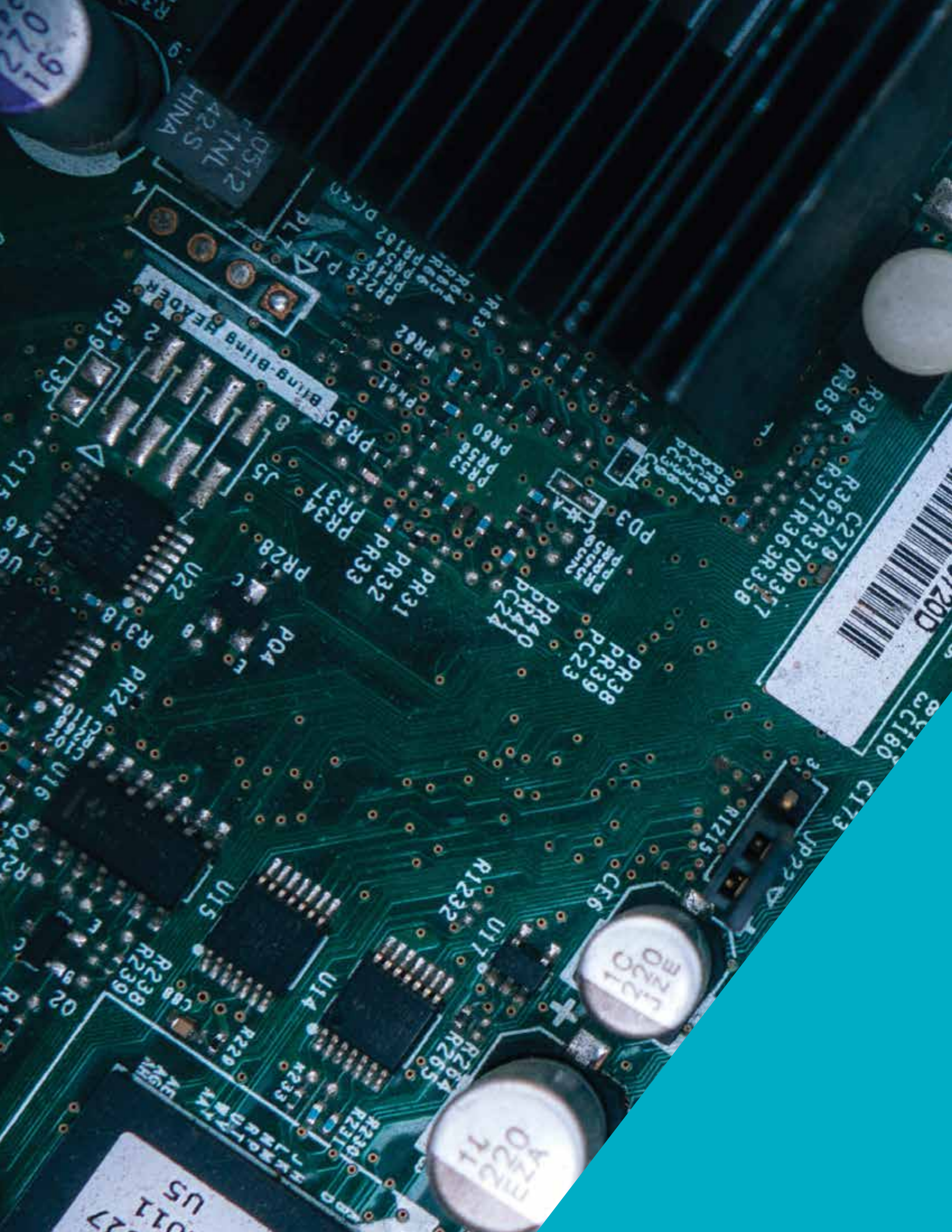
Cybersecurity Budgets

What do they really convey about maturity?

September 2019

co-authored by

S-RM


Billing-Billing Reader

Cybersecurity budget trends

With public and corporate awareness of cybersecurity growing, many companies have been increasing their annual cybersecurity budgets. For instance, according to a survey of executives and IT/security directors from 250 small and mid-size enterprises ('SMEs'), conducted by IT research and advisory company 451 Research, more than 80 percent of the SMEs reported they were planning to increase their cybersecurity budgets by 14 percent in 2019.[1]

Measurements regarding the average percentage of company IT budgets spent on cybersecurity vary depending on the source.[2] For instance, one security spending guide published by technology advisory company International Data Corporation that includes forecasted budget data for over 20 industries around the world, indicated that the industries expected to spend the most on security solutions in 2019 were the banking, discrete manufacturing, and federal/central government industries.[3]

Alternatively, in a 2019 study comparing the budgets of global corporate security decision makers, the technology market research company Forrester found both financial services and public sector industries to be representative of lower spending brackets in terms of the percentage of the overall IT budget spent on security. In its study, Forrester also found that cybersecurity budgets generally could be represented by the three following categories:[4]

- **Up to 10 percent of the IT budget:** included 31 percent of companies in both the financial services & insurance industry and the public sector & healthcare industry.
- **11 to 20 percent of the IT budget:** included 40 percent of companies in the retail & wholesale industry.
- **21 to 30 percent of the IT budget:** included 32 percent of companies in the utility & telecommunications industry.

Up to 10% of the IT budget

31%

financial services & insurance
public sector & healthcare

The financial services & insurance industry and the public sector & healthcare industry are most representative of this bracket, with 31% of companies in both industries spending this amount.

11 to 20% of the IT budget

40%

retail & wholesale industry

The retail & wholesale industry is most representative of this bracket, with 40% of companies in the industry spending this amount.

21 to 30% of the IT budget

32%

utility & telecommunications

The utility & communications industry is most representative of this bracket, with 32% of companies in the industry spending this amount.

Budgets as security indicators

Although the amount of IT budget spent on security is a common focus when discussing cyber risk readiness, based on S-RM's experience advising on cyber risk and responding to cyber incidents, a security budget is not the defining element when preventing or responding to a cyber incident.

This perspective is also supported by companies such as the research and advisory company Gartner, which notes that the money spent by companies on security does not necessarily reflect their security maturity or cyber incident readiness level.[5] Indeed, a company could be allocating a similar percentage of their IT budget to security as its peers, but it could be spending money on unsuitable solutions for its specific situation and still be extremely vulnerable to risk.[6]

There is also inconsistent motivation for either higher-than-average or lower-than average security spending. For example, companies that spend low percentages of their IT budgets on security in a given year may include both unsecured companies under-spending on security and secure organizations that have already implemented best IT security practices that consequently have a more efficient IT infrastructure.[7] Alternatively, comparatively high cybersecurity budgets could either be an indication of budget inefficiencies or that a company is making an initial investment in cybersecurity.[8]

[1]Source: 'Small & mid-size enterprises plan to increase cybersecurity budgets by 14%', Armor Defense Inc, 13 March 2019.
[2]Source: 'Are you spending enough on cybersecurity?', Boston Consulting Group, 20 February 2019.
[3]Source: 'Worldwide spending on security solutions forecast to reach $103.1 billion in 2019, according to a new IDC spending guide', International Data Corporation, 20 March 2019.
[4]Source: 'Is chaos the new normal? Security spending trends to watch in 2019', Recorded Future, 5 February 2019.
[5]Source: 'The role cybersecurity should play in 2019 IT budget planning', ZD Net, 4 September 2018; 'Gartner says many organizations falsely equate IT security spending with maturity', Gartner, 9 December 2016.
[6]Source: 'Gartner says many organizations falsely equate IT security spending with maturity', Gartner, 9 December 2016.
[7]Source: 'Gartner says many organizations falsely equate IT security spending with maturity', Gartner, 9 December 2016.
[8]Source: 'Are you spending enough on cybersecurity?', Boston Consulting Group, 20 February 2019; 'The state of cybersecurity at financial institutions', Deloitte, 21 May 2018.

There is also inconsistent motivation for either higher-than-average or lower-than average security spending. For example, companies that spend low percentages of their IT budgets on security in a given year may include both unsecured companies underspending on security and secure organizations that have already implemented best IT security practices that consequently have a more efficient IT infrastructure.

Cybersecurity budget trends

Although the precise percentage of the IT budget a company spends on cybersecurity may not be a reliable indicator of its cybersecurity readiness, there are several budget-related questions to consider when identifying potential red flags in an organization's cybersecurity budget:

- **Does the organization have a clearly defined and detailed cybersecurity budget?** More importantly than simply how much an organization is spending on cybersecurity, a clearly detailed budget will help inform assessments of where and how resources are being allocated.
- **Has the organization modified its budget following a significant cyber incident?** If an organization has not adjusted its budget following a significant incident, such as by reprioritizing resources or security solutions, this may indicate a lack of awareness regarding its current and future vulnerabilities.
- **Has the organization significantly increased or reduced its cybersecurity budget from the previous year?** As discussed above, there are various reasons why an organization might do this, however it is important to understand each organization's particular motivation.
- **Has the organization increased its cybersecurity budget as part of managing an acquisition or merger?** When a company merges with or acquires another firm, it is important to ensure that its cybersecurity budget includes resources to manage the integration of the different companies' IT systems and security processes.

In addition to budget considerations, there are several additional questions that may be useful to consider when assessing an organization's ability to prevent and respond to a cyber incident:

- **Does the organization have a clear risk management process?** An organization's ability to respond to a cyber incident is not just determined by how much money it spends on security but about whether it understands and addresses its risk exposure and potential vulnerabilities. Ideally, a clear risk management process should indicate how a company's cybersecurity investments are justified and prioritized. When assessing a company's risk management process, the impact and likelihood of a cyber incident occurring should be used to justify the security budget. There are many ways to assess cyber risk-good resources include any of the following frameworks: NIST 800-30, ISO 27005, FAIR, etc. For a cyber underwriter, an ideal insured is one that has reserved cyber insurance to transfer risks that would otherwise require too many resources to mitigate internally or could cause a catastrophic loss to the company.
- **Does the organization implement proactive measures to prevent cyber incidents?** Implementing proactive measures, notably multi-factor authentication, offline and tested backups, and network segmentation, can reduce an organization's vulnerability to or reduce the damage caused by a cyber incident.

[9]Source: 'Don't buy a breach: Ten cybersecurity red flags to look for during MA due diligence', Forbes, 12 February 2019.
[10]Source: 'Don't buy a breach: Ten cybersecurity red flags to look for during MA due diligence', Forbes, 12 February 2019.

To learn more, contact your AXA XL Cyber underwriter.

S-RM is a global consultancy that delivers breach response, ethical hacking, and cyber risk and governance services.

6031_10/2019