Cyber security for digital government leaders

A guide for government senior executives responsible for leading digital initiatives

Ovum
TMT intelligence | informa

Author
Kevin Noonan,
Lead Analyst, Government

An Ovum consulting white paper commissioned by Cisco Systems, Inc.

Summary

Catalyst

Cyber security is now a significant issue for all government entities. It has broad relevance right across the organization, and can no longer be compartmentalized into niche topics such as national security or technical responses to computer hacking. Important as these issues are, they are just one small part of a much bigger challenge that now pervades the operations of government.

Recent events provide a clear wake-up call, and signal the need for a broader enterprise-wide response. Some examples are the US Democrat Party hack, the copying of the personal details of one billion Yahoo users, and the public release of the personal details of 55 million Filipino voters. These are breathtaking numbers, and go to the very core of technology enabled service delivery.

Contemporary cyber security issues need a coordinated response, and one that can engage the enterprise at all levels. The top leadership team has a particularly important role to play.

However, good intentions do not necessarily translate into a call to meaningful action. Many technology leaders are finding it difficult to engage and motivate the rest of the organization on a topic that is typically seen as very dry and technical. It is sometimes even harder to engage the top leadership team in the discussion beyond hygiene factors and simple risk avoidance. As digital initiatives continue to grow in importance, the challenge to engage the top executive team is becoming more acute.

This paper is aimed at Chief Information Officers, Chief Digital Officers, and Chief Information Security Officers, as they work in collaboration with fellow senior executives and with the top leadership team of their organization.

Ovum view

The IT security market has evolved significantly in just a few short years. Long gone are the days when security was all about protecting the hardware and software assets located within the datacenter. Today, much of an organization's processing already happens outside the datacenter. Perimeter security has become just a small part of the overall challenge. Smart cities, mobile devices, cloud computing and a myriad of small devices from the "Internet of Things", have together driven security out to the very edges of the network and into cyberspace.

Today's cyber security challenges require a more **holistic solution** because digital initiatives are quite literally happening *everywhere*.

But this is far from the end of the story.

The emerging security challenges for the government sector can no longer be dealt with from a purely technical perspective. For example, the recent US presidential race saw cyber security and shadow IT become a significant issue in the election of a national leader. Claims about Hillary Clinton's use of a personal email server for official emails became front page news. The issue resonated with a community that is now much more technologically aware.

However, despite this profound evidence, many government sector leaders fail to make the connection between changing public expectations and the underlying need for a security culture within their own organization. Cyber security is now as much a senior leadership challenge as it is a technical challenge.

Increasingly, the community is looking at technology as a normal part of the processes of government. Good government should be competent, predictable, trustworthy and open.

If a government enterprise can deal with cyber security in a way that *meets community expectations*, then the overall standing of **government is enhanced**.

If a government is seen to *act recklessly or fails to meet community expectations*, then the overall reputation of **government is damaged**.

Key messages

This report is not intended as a detailed technology roadmap. Instead, it focuses on five key senior leadership issues (Figure 1). Each issue is supported by statistical research and practical case studies that resonate at an executive level.

Top 5 cyber security recommendations for digital government leaders

A structured approach for senior leadership team to drive cyber security across the enterprise

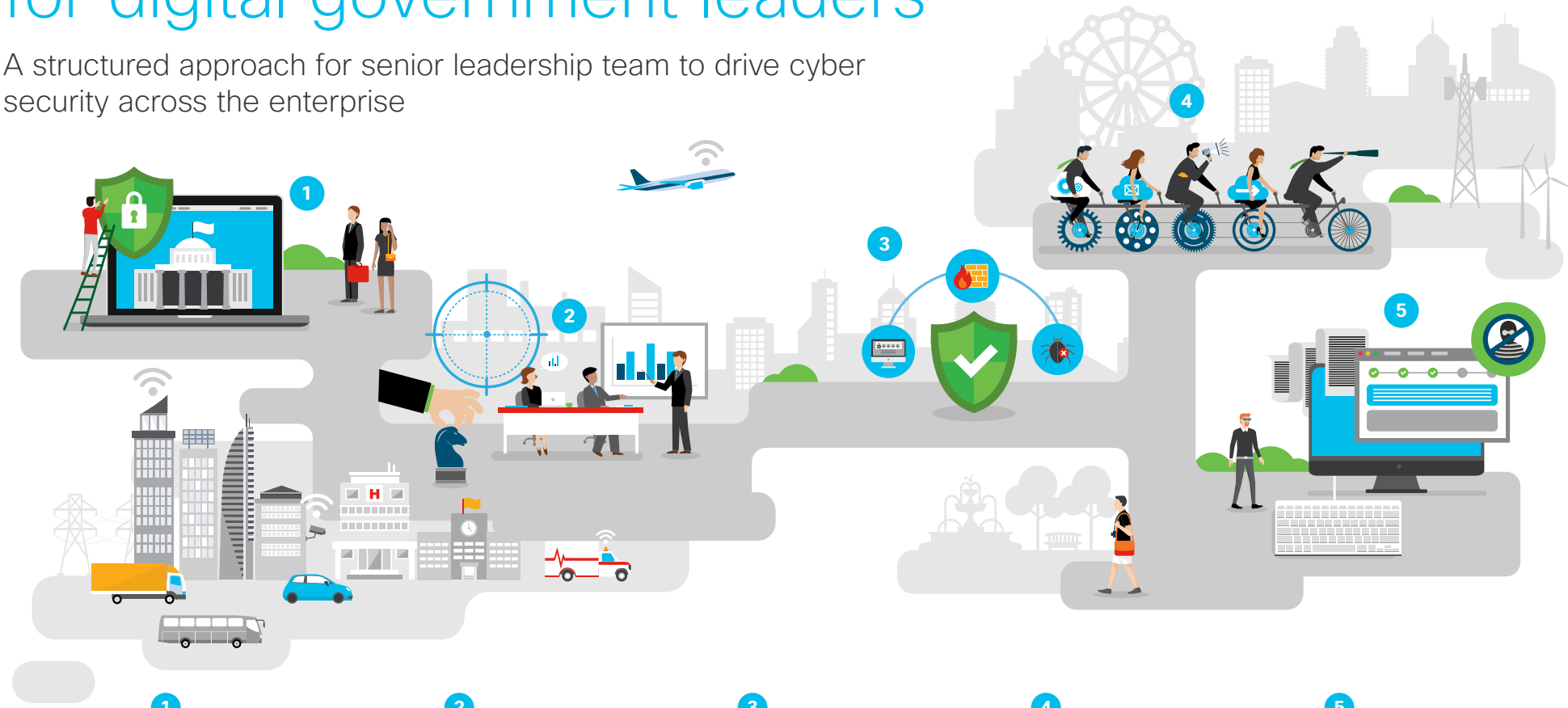


Figure 1: Ovum's recommendations to top 5 leadership concerns

1

Put security at the foundation of digital government initiatives

A successful digital strategy must start with cyber security at its foundation. Digital strategies are more likely to fail if they simply graft security on as an afterthought.

2

Provide more focused senior executive leadership

The executive leadership team has an important part to play in driving an approach that specifically addresses the needs of the government sector.

3

Rethink your IT security architecture to address contemporary challenges

The industrialization of hacking requires a much more sophisticated and more integrated security response. Older point solutions are fast becoming ineffective.

4

Leading change is about leading people

Cyber security is as much about people and leadership, as it is about technology and tools. Successful strategies need to take account of the realities of leading people.

5

Take a balanced scorecard approach for managing security outcomes

The senior executive team needs to have a high-level scorecard to focus attention on the issues they must manage and track.

Recommendations

Recommendations for
Digital government leaders

Cyber security is no longer an issue that can be effectively dealt with by technical risk mitigation alone. Digital government is now good government, and technology is an inseparable part of everything we do. Cyber security needs to be treated no differently, as it is now core to maitaining the trust of the community. It can no longer be delivered effectively if viewed only from a technical perspective.

Recommendations for
Vendor partners

Vendors have a great deal to offer in dealing with contemporary cyber security challenges. As these challenges become increasingly complex, there is a growing need for architected solutions that reach the very edges of the network and beyond. More than ever, the government sector needs assistance from trusted industry partners, rather than just suppliers of disconnected point solutions.

Put security at the foundation of all digital government initiatives

> Our past ideas about information technology are no longer sufficient to meet expectations of the digital era

The emergence of the digital enterprise is one of the industry's hot topics. Today, it is almost impossible to pick up a newspaper or follow an online news feed without some discussion about technology and change. Ovum research has found a clear shift in digital government priorities, as the realities and challenges of digital transformation in a government context begin to bite. In the past, it may have been possible to maintain a minimalist view of digital government – that it was just the next stage of technology evolution, or perhaps that it was just a market aberration unlikely to impact the relatively stable world of government administration. However, this minimalist view has proven to be incorrect.

Government digital initiatives have moved on from early implementations that focused on simple apps and website consolidation. These quick wins were essential for building momentum for change, but their job is now done. However, some have been lulled into a false sense of security by the relative success of delivering the quick wins. Digital government is becoming an increasingly complex journey. Today's challenges require a stronger focus on new governance arrangements and whole-of-enterprise cultural change.

Figures 2 and 3 draws on a large survey of government executives globally, and they provide a clear assessment of just how much the government market has matured. The early bickering about job titles and internal structures (Figure 2) has all but disappeared in the priority rankings (only 1.3% rate this issue as their top priority).

Today, the big issues are all about delivering real outcomes from digital government, and in that context, it is noteworthy that cyber security now takes top position:

- 20.1% rate cyber security as their top issue, while 52.3% rate it as one of their top three challenges. Security has become a big issue as government constituents grow nervous about the ability of the government sector to look after their data. The community is increasingly judging governments on demonstrated outcomes, and secure rhetoric can be easily demolished by a single high-profile failure.

The second top challenge for government managers is skills (16.91% rate it as their top issue, while 35.7% rate it as one of their top three challenges).

Ovum interviews with government senior executives confirm there is a growing shortage of skills to meet emerging needs, particularly around cyber security.

Lack of funding comes in at fourth position overall but ranks very high in direct interviews with executive respondents. While only 13.3% rated it as their top issue, 49.5% rated it as one of their top three challenges).

Source: Ovum – ICT Enterprise Insights 2016/17 Public Services: Government

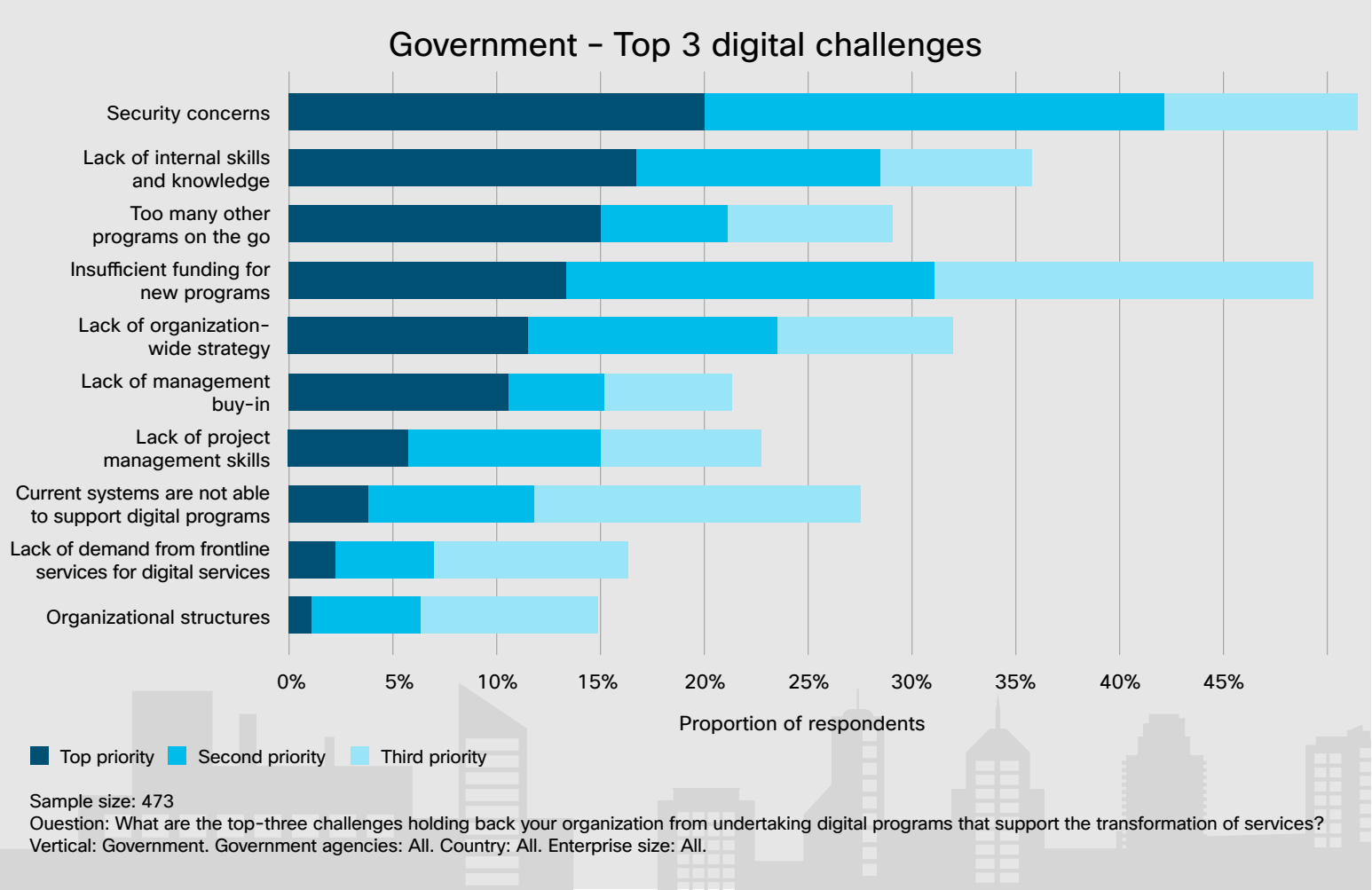


Figure 2: Government – Top 3 digital challenges

Source:
Ovum – ICT Enterprise Insights 2016/17 Public Services: Government

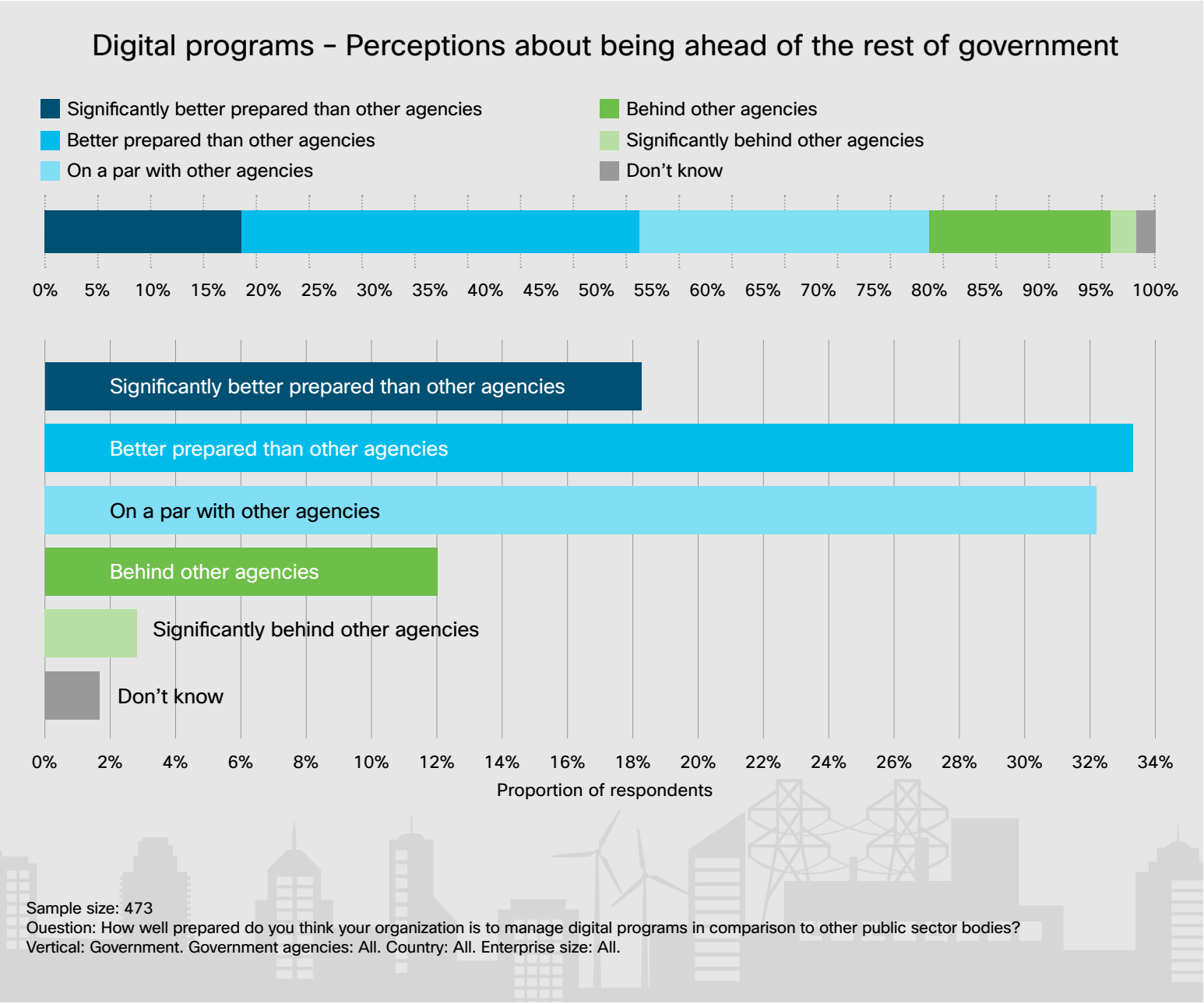


Figure 3: Perceptions about being ahead of the rest – government

The tough realities of digital government have not yet been fully accepted at a leadership level. Figure 3 indicates that government executives tend to rate their digital preparedness very optimistically when comparing themselves against other government enterprises. The survey found that only 15% admitted to being less prepared than other departments and agencies, while 51% believed they were doing better than everyone else, and 32% believed they were on par with others. Of course, it is statistically impossible for everybody to be better than everybody else. There is therefore a significant gap between perceptions of management preparedness and reality.

As digital agendas continue to grow and mature, an important relationship is emerging between the relative success of cyber security and digital initiatives (Figure 4). Government departments that have a rudimentary approach to digital initiatives, tend to fall well short in meeting contemporary community expectations. However, as digital government initiatives grow and mature, the proliferation of online facilities tends to act as a honey pot for potential hackers.

If a government enterprise fails to develop an appropriate cyber security strategy, the result could end in high profile failure.

If, on the other hand, *significant attention is given to cyber security, without the corresponding development of digital initiatives*, the result is likely to be public frustration with government services that are seen **to be secure but ineffective**.

Source: Ovum

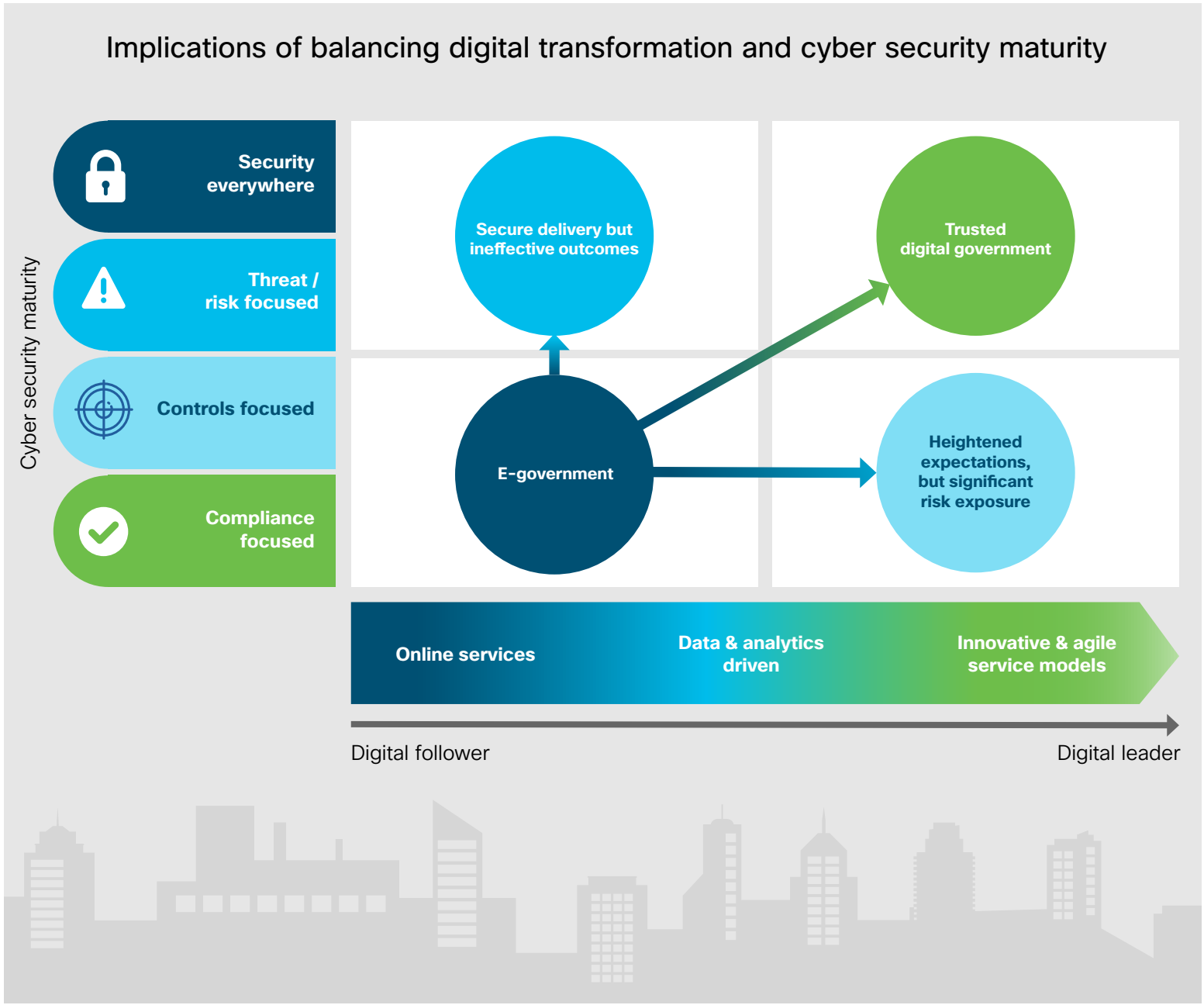
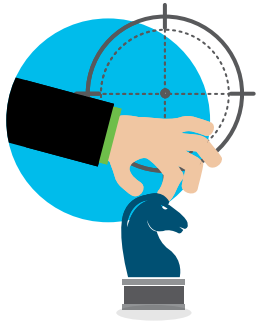


Figure 4: The implications of balancing digital transformation and cyber security maturity



Provide more tightly focused senior executive leadership

The government sector has different business drivers to the private sector

Much of the contemporary IT management literature about cyber security and digital transformation, tends to focus on market competitiveness as a key driver for change. Essentially, the argument goes like this: “If your data is hacked, then all the adverse publicity will enable your competitors to steal your customers.”

This is a sensible and realistic argument for the private sector. However, the government sector typically does not have a profit motive and is rarely driven by competitive market objectives. Instead, the government sector exists to serve, protect and educate their citizens, particularly in policy areas that cannot be performed by the private sector. Government most often operates in the area that economists refer to as “market failure”. This is where competitive market forces are unable to operate effectively, and government must step in to deliver specific policies and services. Frequently, government operates as a monopoly service, where citizens are compelled by law or by regulation to deal with government in specific ways.

But the lack of competitive forces does not imply at all that governments can act without regard to public opinion. In fact, the opposite is true.

The government sector cannot operate without the **help** and **support of the community**.

In a 21st century digital world, negative community feedback can be *swift* and *blunt*. Community confidence can be lost quickly and can take a long time to rebuild.

Cyber security needs to come out of the back room

Information technology is no longer a back room internal function for supporting the business of government.

> Increasingly, technology is becoming **core** to the way the business of government is *conceived, legislated, delivered, enforced and measured*.
>
> Our understanding of digital government is maturing quickly, and is increasingly at **the heart of government reform**.

For example:

- A growing number of government functions are already being performed either in part or exclusively online
- Advanced analytics has become a fundamental part of government decision-making
- Artificial intelligence is already beginning to augment or replace some of the value-added activities traditionally performed by white collar workers

Just as information technology has come out of the back room, so too must cyber security.

Although cyber security skills are becoming increasingly specialized and highly technical, these skills alone are not sufficient to deliver an appropriate government response to the need for enterprise-wide security. Senior executive engagement needs to go well beyond passive sponsorship, and instead become more directly involved in clearing the path to ensure good outcomes. Overall accountability for government outcomes must rest with the top leadership, and the CIO/CDO and CISO need to be a key part of that team.

Case study

The 2016 denial of service attack on the Australian National Census

In past years, the Australian National Census had largely been a manual data collection exercise. Hardcopy survey forms had to be manually delivered to each household in the country, and sometime later, all these forms had to be manually collected before data entry. The 2016 census planned to change the entire process so that it was primarily conducted online. Following an earlier number of successful trials, there was great confidence that the system would work well. However, on census night the system was hit with a number of Denial of Service attacks. Eventually the entire system had to be brought down and it took days before the integrity of the system could be assured.

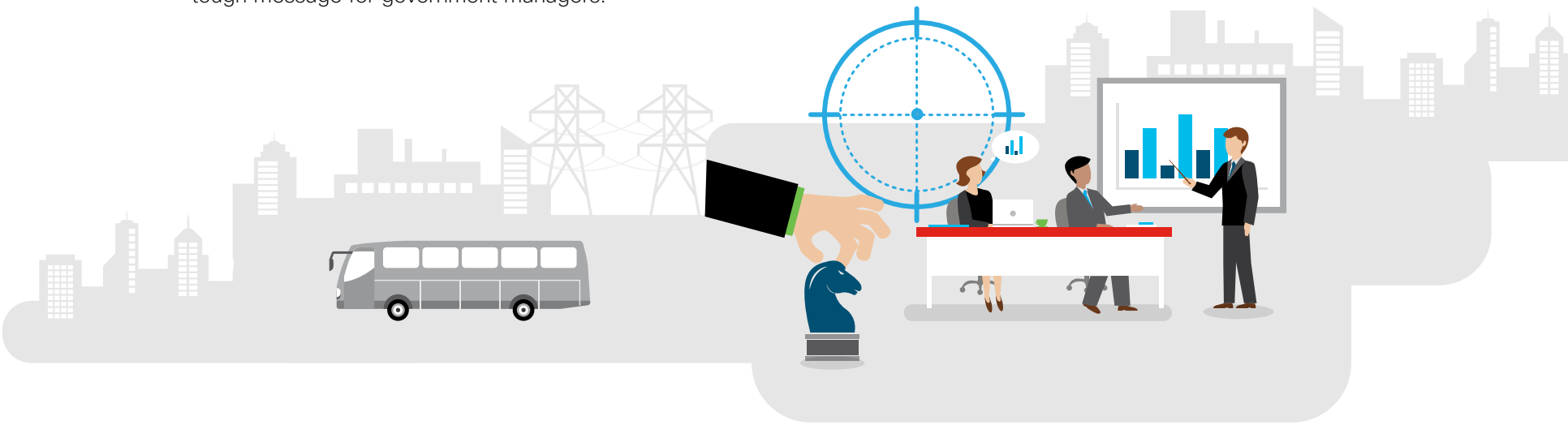
From a technical perspective, the impact of the DDOS attacks was very limited. No data was lost, no government IT infrastructure was compromised, and the Census was eventually completed. Indeed, the Census did achieve an impressive 96.5% response rate, with 58% of households participating online.

However, the damage to public credibility had already been done. The Census project had gained an unofficial Twitter hashtag #CensusFail, and negative public commentary through social media quickly took over from the official government messaging. It was no longer a situation of government informing the public about the value of the new system. Instead, the public was informing government about its unhappiness and loss of confidence.

The Census had previously relied on its public reputation, to ensure the data they collected was reliable and used confidently by government and industry. This time, Government surveys found the Census had taken a significant blow in the eyes of the public. A massive 42% of the public saw that to some extent the Census had been a failure, and 33% believed that to some extent the data collected by the Census was unreliable.
In the aftermath, the Government commissioned a high-level independent review. This report focused on the broader implications for government administration, and delivered a tough message for government managers.

The report's executive summary commenced: *"The Australian Government's new paradigm for online engagement and services is not coming. It is already here …. Cyber security is about availability of services and confidence in government in a digital age. And the public's confidence in the ability of government to deliver, took a serious blow, more so than any previous IT failure …. But crucially important is the need to understand how the Census got to the point where the cyber security arrangements brought into question the trust and confidence in a fundamental government service. The public's lack of confidence will linger".*

The report recommended that government senior executives should attend a "cyber boot camp", so that they could better understand the broader implications for government senior executives and the important part they should play.



Rethink your security architecture to address contemporary challenges

> The industrialization of hacking requires a much more sophisticated security response

While the practice of malicious computer hacking may be as old as the IT industry itself, the scale and nature of hacking has changed significantly in recent years. Long gone are the days when hackers were little more than amateurs who were intent on creating minor disruption to business operations (Figure 5).

Source: Cisco

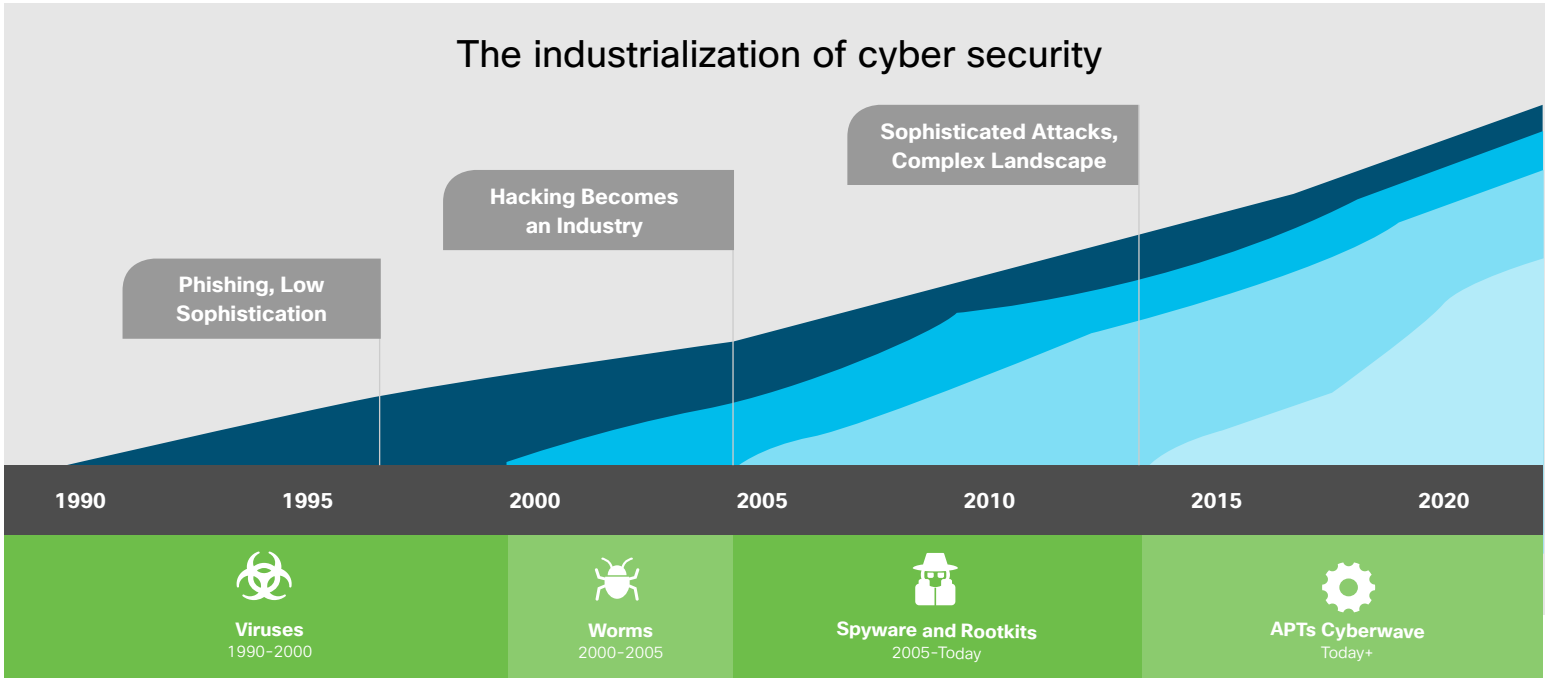


Figure 5: The industrialization of cyber security

Cyber security has turned into an industry with all the sophistication and skills of a fast developing industry sector. While amateur hackers still exist, today's hackers are often professionals. They are now just as likely to be skilled workers who arrive at a regular job every day. They are typically well paid and are well-equipped. However, their employers are anything but typical. Their employer could possibly be an organized crime syndicate, a foreign intelligence service, or a specialist company contracted to undertake industrial espionage. Many hackers now use modern techniques for rapid application development and have ready access to online markets for generic off-the-shelf malicious code.

Hacking has matured to such *a level of sophistication and industrialization*, that no enterprise can hope to mount a credible defense if they are still using legacy security tools acquired through piecemeal procurement.

Contemporary security tools need to look across the network in a more consistent way. The tools must provide an **industrialized solution to an industrialized problem**.

There are three key selection criteria for contemporary cyber security tools:

- **Simple:**
  Network complexity should be borne by the security solution, not by the operator
- **Open:**
  The solution should be able to evolve and grow over time without the requirement for significant changes to the underlying architecture
- **Automated:**
  The security tools should use advanced techniques to learn and respond to any suspicious activity without needing to continually wait for human intervention

The top leadership team has an important guidance role, given an increasingly complex set of digital challenges

Despite the increased sophistication of cyber security defenses, the odds of success are still weighted in favor of the attacker. Cyber defenses need to work successfully day after day, whereas the cybercriminal needs to be successful only once.

In today's cyber security environment, it is impossible to guarantee that an adverse security event will never happen. The important question for the top leadership team is no longer "are we secure", but "is our security posture fit for purpose".

Every government entity has a different risk profile and its security posture must be sufficient to meet the needs of that organization. If security is too tight, the efficiency and effectiveness of the organization is compromised. If security is too loose, the organization will be an easy target for sophisticated attackers, and the executive leadership of the Department will be exposed to criticism.

A fit for purpose security posture should not singularly focus on preventing possible attacks, as it would be naïve to do so. A more prudent management strategy should take account of the full range of activities necessary to deal with the entire Attack Continuum (Figure 6). A successful posture should not only minimize the likelihood of attack, but should also put robust plans in place to minimize the damage if an attack is successful.

Source: Cisco

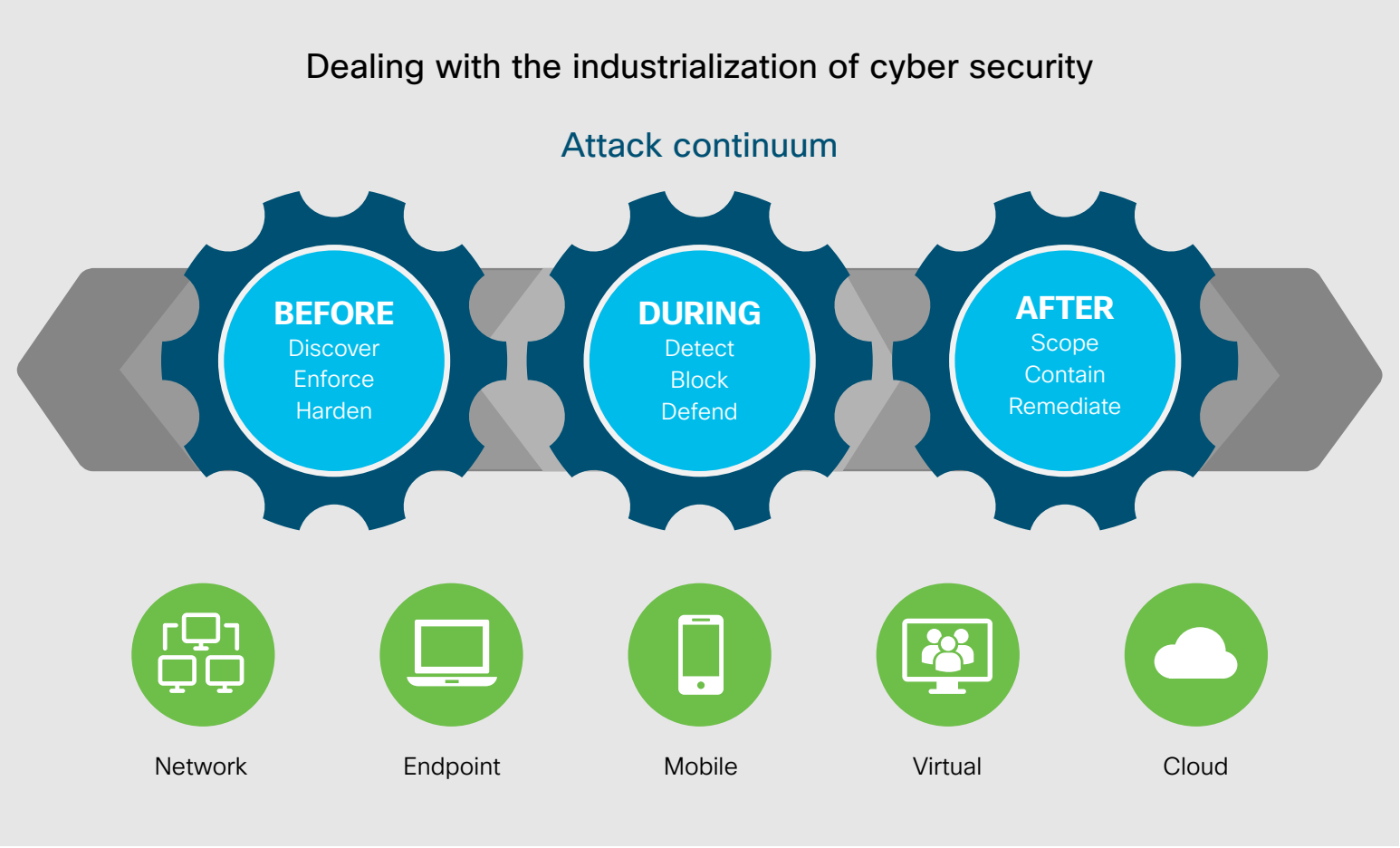


Figure 6: Dealing with the industrialization of cyber security

The executive leadership team needs to focus its attention on five key questions:

1. **Does the security architecture aim to stop threats at the edge of the network?**

Successful hackers frequently start with small security exposures, and leverage these to find or construct even bigger exposures. Devices at the edge of the network tend to be easier targets. These may include cloud services, mobile devices, Internet of Things, shared services delivered through external partners, and outsourced IT services. It is therefore crucial to prevent unauthorized access at the edge, before a potential attacker has a chance to gain access to core systems.

2. **Can the architecture protect users wherever they work?**

The nature of work is changing rapidly. It can no longer be assumed that work will be performed by traditional employees or in a traditional office environment. Today's worker could easily be performing legitimate work anywhere, at any time, and on any device. The security architecture should therefore not place unreasonable limitations on how or where work is performed.

3. **Can the architecture adequately control who gains access?**

As the number and variety of activities on the network continue to grow, identity and access management is becoming a significant issue. The technical mechanisms for dealing with this problem are becoming increasingly challenging and complex. Notwithstanding this, the executive team should satisfy itself that appropriate measures are in place to deal comprehensively with identity.

4. **Is the security architecture simple and integrated?**

The executive team needs to understand potential risks to the enterprise if it is to adequately deliver on its governance responsibilities. Complexity is no longer a measure of effectiveness. The executive team needs to be able to clearly understand the broad cyber security structure and direction, and receive regular updates on performance, challenges and potential exposures.

5. **Can security issues be discovered quickly and contained effectively?**

Cyber security reports should contain metrics for any adverse activity and response. Reports should discuss the full attack continuum (Figure 6)

Case study

Addressing the management challenges due to growth and complexity

A city in Japan needed to concurrently deal with a variety of security-related challenges:

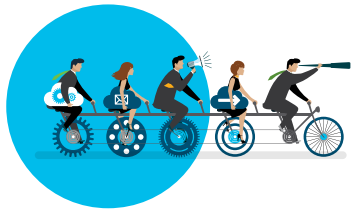
- There had recently been a number of changes in government policy, including the introduction of a national identification number, as well as a number of pension related changes. Due to changes, the city needed to significantly step up its security posture to match its changed IT risk profile.

- The city also needed to manage significant growth in its IT infrastructure. This was particularly driven by a five-fold increase in the number of devices connected to the network.

At the same time, the city needed to manage its ongoing operational costs, particularly the growth in IT operations staff. It was simply not possible to continue to increase staff numbers in line with the growth in size and complexity of the systems they were supporting. A different approach was needed.

The city chose to implement an integrated security solution through a single prime supplier, rather than individually choosing products from different suppliers.

This approach delivered significant benefits that went far beyond the obvious benefits in simplifying procurement and contract management. The city found a single, architected solution delivered a more holistic approach to managing network security. This enabled the city to manage its security architecture more seamlessly and grow with the city as new requirements emerged. It also provided a more effective way of minimizing growth in operations support headcount.



Leading change is about leading people

> Cyber security is as much about people as it is about technology and tools

It is now a well-established fact that many security breaches succeed through human engineering – by exploiting simple human vulnerabilities. Even the best security systems can be circumvented by leveraging the back-door exposures available to internal staff, suppliers or clients.

However, security exposures do not always occur due to *simple errors and oversights*. An increasing number relate to staff actively circumventing what they see as **impractical procedures and governance**.

These issues *cannot be solved* through simple staff instructions or information campaigns. Instead, they require a **pragmatic understanding of the way bureaucracy works in 21st century organizations**.

Through a series of executive interviews, Ovum found many examples:

- Business managers are drawing on their ingenuity and their internal knowledge of administrative procedures, to "game" the organization's rules to achieve what they see as a pragmatic outcome
- Business managers are creating security exposures, not through any malicious intent, but through simple ignorance of the underlying technology

Case study

When rhetoric does not equal reality

One CIO related to Ovum the following story:
"Notwithstanding all our existing security procedures, who do you think would have incorrectly sent secure data to his tablet device and then proceeded to lose that tablet device?" It was the CFO.

The CIO went on to remark with a wry smile, "Sometimes 'remote wipe' can be a valuable tool of last resort".

Case study

The increasing use of shadow IT

A government department once contacted Ovum to ask for advice about eradicating shadow IT. The department had specific concerns about the increased security exposure created by the unapproved use of Cloud services.

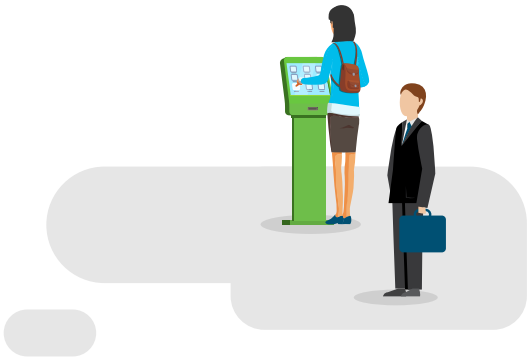
When Ovum asked what the organization had done so far, the senior executive in charge replied that he had sent out a number of all-staff emails instructing staff to stop using it. However, when Ovum asked about success rates, he admitted the emails had just made the problem worse. All that was achieved was to publicize an effective way of circumventing existing IT governance. In effect, the all staff emails achieved the opposite of what he had set out to do.

Implications for government managers

Sometimes, driving security is not only about logic, but also about pragmatically understanding the subtleties of organizational culture. Adherence is no longer driven just by hierarchy. Instead, there are four complex forces at play: management, leadership, governance and culture. When these four forces are out of alignment, culture typically prevails.

In this organization, there was no problem with management structure, however its governance was weak and impractical. The organization's staff knew very well how to circumvent its internal bureaucracy; therefore, its internal culture prevailed. The solution was not to send out more all-staff emails but to deal with the realities of the prevailing culture. In this organization, what appeared to the organization as shadow IT, was actually internal innovation looking for some better leadership.

It is interesting to note that in unrelated Ovum discussions with two government departments in New Zealand, both noted that the amount of shadow IT had significantly decreased as their government digital programs gathered pace. Staff followed the rules when the path was made easy for them to follow the rules.

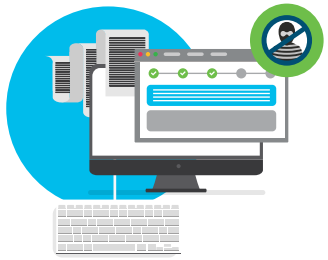


Case study

Ingenuity will prevail, so why not put it to use

Ovum interviewed a manager in a government department where they had strong requirements for data security. When asked about the use of personal devices, the manager immediately replied that the department's security rules did not permit personal devices for official use. Ovum then asked if the manager owned a smartphone, and if the manager ever needed to send work to his phone or tablet. "Of course," he replied, "sometimes you just need to get the job done."

In this manager's mind, he was doing the right thing: he was simply taking personal initiative to deal with what he saw as an unworkable situation. When asked if he would comply with more workable procedures, and invest some effort into helping to create new procedures, the manager responded with equal enthusiasm. Unfortunately, this organization was already caught in a spiral of increasingly difficult to use IT services, and increasingly tightened internal rules.



Taking a balanced scorecard approach to security outcomes

> It is not possible to shift executive accountability

The senior executive function is ultimately accountable for delivering Government outcomes. It matters very little whether a security exposure came from a complex hacking event, or an unexpected event originating with an external service provider, or even from an internal staff member simply not following the rules. The hard reality of accountability is still the same.

The executive team must find practical ways to strike a balanced approach to technology leadership, and measure their own success. Security procedures must be sufficiently tight to ensure the ongoing confidence of the community. However, security rules cannot be so restrictive that they stifle innovation or the efficient running of the enterprise. Given the growing number and the increasing complexity of cyber-attacks, balancing these realities may present what appears to be an impossible proposition.

Engaging the executive leadership team

Cyber security is an increasingly complex and specialist activity, and many of these activities need to be performed by specialist internal staff and suppliers. While a growing number of Departmental Secretaries are very comfortable with information technology, discussions about cyber security can sometimes become mind numbingly difficult, and may appear to be quite disconnected from the other issues typically managed by the top leadership team.

It is crucial that the executive leadership function should not be bogged down in the technical detail about how cyber security tools are assembled and implemented. Instead, **the executive team needs to remain focused on the issues it is best equipped to manage**.

It is clearly the role of the senior executive to lead and guide cyber security outcomes across the organization, but also to manage any issues down to a sufficient level of detail. It is a constant challenge when trying to achieve this balance, both efficiently and effectively.

Case study

A bridge too far

In one government department, the CIO and CISO were both having great difficulty getting time with their top leadership team to discuss cyber security. As a result, they decided to undertake an education campaign, drawing on some of the horror stories from around the world, to demonstrate what can happen when executives do not pay sufficient attention. Their education campaign succeeded, but not in the way they expected. The executive team responded by demanding a very risk averse strategy across the entire department.

Meanwhile, the Chief Digital Officer was given the task, by the same executive team, to drive an innovation agenda across the organization, to encourage staff to become more agile and more skilled at managing risk.

When the staff received these mixed messages, both messages were interpreted as just more management noise. So, staff ignored both messages. After much adverse feedback, the reputation of IT also began to suffer.

In this encounter, everybody lost!

There are some important lessons:

- The leadership team was not given a workable mechanism to manage and balance these messages
- The leadership team had no way of measuring success
- An excessive focus on risk avoidance, had itself created greater risks

An executive balanced scorecard for leadership in cyber security

The table on the next page below provides a high-level balanced scorecard for the top leadership team. There is a checklist of ten questions, each of which should be rated on a scale of one to ten.

This is not intended to be a comprehensive checklist, as such an undertaking could easily span many pages. Instead, its purpose is to draw attention to the big questions that require executive consideration, and possibly executive intervention. Ideally, for each of the ten questions, there should be a policy or strategy that drives change and measures success.

High-level balanced scorecard for the top leadership team

PEOPLE (Score 1)

1. Our staff see security as an intrusive overhead
2. “Security concerns” are frequently used to shut down discussion about innovative ideas
3. Some staff follow the rules, but others are just “gaming” the rules. Shadow IT is out of control

PEOPLE (Score 10)

1. Our staff believe current security level is appropriate and well balanced
2. Our cyber security processes provide a framework that empowers our staff to do more
3. Our staff adhere to the security rules. We understand their implications for maintaining community trust in government administration

PROCESS (Score 1)

4. We struggle to meet government cyber security standards
5. Cyber security reports contain a lot of data, but executive management doesn’t feel informed or confident
6. The Department has little understanding of the way security is managed by its partners and suppliers
7. We do not expect a security related event will happen to us

PROCESS (Score 10)

4. These standards our just the beginning. It is all about overall process improvement
5. Managers receive regular reports focused around risk, processes and outcomes
6. The Department is confident that its partners and suppliers are not creating extra security exposures for our systems
7. We have a clear plan and it has been tested. This includes a war room, remediation procedures and public messaging

TECHNOLOGY (Score 1)

8. We have a lot of disconnected security tools and rules. Each delivers part of the solution
9. Our technology suppliers just deliver tools and services
10. The Department has little understanding of the way security is managed by its partners and suppliers

TECHNOLOGY (Score 10)

8. We have an orderly, architected approach to cyber security, focused on clear organizational outcomes
9. Our technology suppliers are our trusted advisors
10. We know why our data is being collected, where it is stored and how it is being managed

Appendix

An Ovum Consulting White Paper commissioned by Cisco Systems, Inc.

Methodology

Ovum undertook a series of interviews with government senior executives as revision of published research and documentation.

Further reading

ICT Enterprise Insights – 2016/17 Public Services: Government, PT0080-000005 (October 2016)
2017 Trends to watch: Security, IT0022-000808 (October 2016)
2016 Trends to Watch: Security - Cybersecurity has a mandate to protect businesses and users, IT0022-000522 (October 2015)

Author

Kevin Noonan, Lead Analyst, Government
kevin.noonan@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Americas Headquarters
Cisco Systems, Inc
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**