Securing Digital Government

Addressing five common security challenges for local government organisations

Introduction and purpose

A more connected world offers many advantages in terms of information sharing and communication.

But by its very nature, being more connected introduces new threats, as organisational boundaries become blurred. At the same time, the tools used by attackers have become more sophisticated but also easier to use.

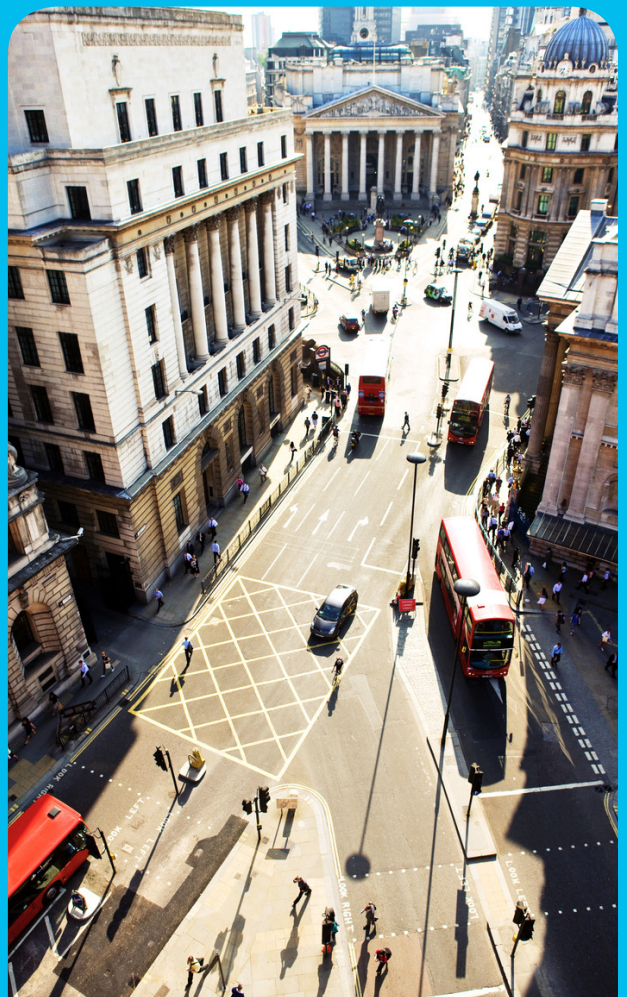
This change in the threat domain is a constant challenge for all organisations, not least those delivering public services. In addition, the increasing prevalence of new threats, such as ransomware, demonstrates that attackers are adapting at a faster pace and organisations are struggling to respond.

In this document, we set out five common security challenges facing local government organisations. In response, we propose that security should be treated as a system and blended into an architectural approach that more directly aligns business needs with the technology domain. And finally, we demonstrate solutions that help to create that security system, offering the best possible mitigation.

As local government organisations embark on digitally transforming the delivery of their public services, new partnerships, combined with a greater need to share systems and information, open up the threat landscape even further. Furthermore, the Internet of Things (IoT) is resulting in billions of elements becoming connected, from cars to trees and buildings, with this revolution situated at the heart of smart and connected community projects. Despite the many benefits this will bring, it will also introduce new 'back doors' and security threats, which must be considered as much a part of the security domain as any IT system.

Ongoing budgetary constraints are driving local authorities to change their public service delivery processes, but this transformation creates risk. Yet disruption to these digital systems is no longer acceptable. Any loss of system availability can have a significant impact on an organisation's reputation and can also damage public trust. In addition, under the EU General Data Protection Regulation (GDPR), which is now in force, failure to report breaches of personal data to the relevant supervisory authority within 72 hours will now incur financial penalties.

Lack of funding is also resulting in skills shortages, with the security function rarely performed by dedicated personnel. This often results in a reactive rather than proactive response by employees who have to perform this role in addition to their main job specification.



Contents

Striking a balance between data accessibility and data protection is essential, yet traditional approaches to information governance and security are failing to meet this challenge of dealing with a rapidly changing threat and business landscape.

Security models focused solely on hardening the network perimeter and endpoints are failing and can no longer be relied upon.

Five common security challenges for local government organisations

The evolution of the threat domain has meant an increase in the number of vectors that need to be considered, along with the ever-present threats that are typically procedural (such as patching), or human behaviour related. Here we identify five threat vectors that are common to all local government organisations.

1. Malware

Malware represents one of the greatest cyber threats to all organisations, including local government. The near exponential rate at which new malware variants are released, combined with the inherent limitations of the current signature-based defences, are resulting in a high risk of infection.

The use of ransomware, for example, continues to grow. The cause of several high-profile cyber incidents, it remains an easy route for criminals to extort large sums of money from their victims. In addition to financial risks, a ransomware infection can have a significant impact on local government organisations, particularly if essential business systems are infected, rendering them unusable until they can be recovered.

A robust backup and recovery procedure continues to be one of the best lines of defence against ransomware. However, in many cases the risk of initial infection can also be reduced through a combination of improved user education and the deployment of defensive controls that don't simply rely on signatures alone.

2. Multiagency working

Digital transformation programmes within local government are driving significant changes in the design and delivery of public services, resulting in reduced cost and improved efficiency. However, these programmes also require greater collaboration, both within the public sector and with new private sector partners.

Contents

This increasing need to work collaboratively brings with it a range of security challenges. At policy and governance levels, clear agreements and processes must be established, for secure information exchange purposes, and to ensure that data is shared only when there is a genuine and necessary need.

Multi-tenancy of public sector buildings is a key aspect of multi-agency working, especially with the advent of the One Public Estate programme. However, it is not uncommon for shared workspaces to be equipped with physical connectivity to each distinct agency. This means that visiting staff members must be able to connect to their 'home' network manually. As this requirement increases, this approach to providing connectivity is not manageable and must be replaced by dynamic 'hot desking' facilities or reciprocal wireless access to ensure that any user is assigned the correct access privileges based on a set of user credentials.

3. Incident response preparation

Historically, security solutions were designed fundamentally to prevent threats from infiltrating the network. However, the sheer complexity of modern networks, coupled with the sophistication of malware, means this approach is no longer viable.

Today, the question is no longer if a security incident will occur, but when. The increasing reliance on digital technology in the delivery of public services means that local government organisations must implement robust incident response plans.

In the face of the very real risk that a breach will occur, such plans cannot be isolated to the IT function. The potential impact a cyber attack could have on an organisation means that incident response plans must align to existing business continuity plans and should also take into account the processes for engaging external professional support and law enforcement agencies. These plans should also consider the implications of the mandatory breach notification requirements of GDPR, referred to earlier. Finally, to remain effective, any incident response plan must be regularly tested and be subject to continual refinement based on the outcomes of each test.

4. Cultural challenges

Culture remains a perennial challenge for the cybersecurity domain, and this is especially true across the UK public sector. The majority of public sector staff are deeply committed to their work, but when faced with poorly designed IT systems, they will find workarounds or alternative approaches to achieving a given outcome. Such workarounds may, however, inadvertently lead to insecure behaviours such as the use of so-called shadow IT – unsupported and unsanctioned applications, which are often cloud based.

Contents

It is not uncommon for staff to adopt unauthorised cloud-based email or file-sharing applications. This type of activity often goes unnoticed, leading to risk of infection from malware, loss of data, and potentially even breaches of data protection legislation. Other examples include the use of well-known consumer messaging and video-conferencing applications.

Rather than blocking this behaviour, it is important to understand which business need is not being fulfilled by current solutions and to develop a secure and sanctioned method for achieving the desired outcome. Furthermore, it is important to foster a culture of security within the organisation. This must extend beyond annual training and should include the introduction of security champions who can act as local points of escalation and sources of best security practice.

5. Executive leadership

Not unlike the issue of culture, executive leadership is a familiar challenge for organisations attempting to build a comprehensive cybersecurity programme. Overall executive leadership is critical for developing and implementing a comprehensive cybersecurity strategy. All too often however, security is perceived as a technical problem and is quickly delegated to the IT department.

When handing over this responsibility, executive leadership teams often provide limited guidance to the IT team regarding which business applications are the most critical. This can lead to a lack of clear understanding of risks that need to be managed – which in turn results in a poorly applied set of controls and, at worst, elevated levels of risk through inadequate protection of an organisation's most sensitive assets.

Contents

It is critical, therefore, that executive teams clearly understand the potential impact of a cybersecurity breach. It could, for example, result in the loss of confidentiality, integrity, or availability of critical public or internal business systems. This could lead to reputation damage, loss of public trust and compromise an organisation's ability to deliver essential public services. To support executive understanding, IT teams need to improve their ability to explain risk in a nontechnical way and seek strong business guidance to prioritise investment.

Adopting an architectural approach to security

We have identified five important security considerations for organisations to consider as they digitise the delivery of their public services.

While each one can, of course, be addressed in isolation, the most reliable approach is to view all your security needs as one complete system.

Taking an architectural approach means treating security as an end-to-end system, rather than a distinct set of individual components. This overall system should be easier to manage as well as capable of sharing vital contextual and threat information, to deliver a more responsive and effective outcome. This approach can also help address cyber skills shortages and a lack of available resources for investment in people, processes, and training.

Such an approach should adopt the following guiding principles:

- A policy shift that considers security to be an enabler.
- Organisations must accept that it is no longer a case of if but of when a security breach will occur.
- Security controls must transcend the traditional 'block' approach taken and instead focus on improving detection and remediation times.
- Security should be developed as a system. Distinct components should not operate in isolation; rather they should integrate to provide more accurate threat detection and reduce management complexity.

Why an architectural approach?

An architectural approach is fundamentally driven by the needs of the business. By first identifying the information assets and systems that support the organisation, an assessment can be performed to determine the relative impact when a compromise occurs.

Contents

Compromise can take place across all three aspects of information security: confidentiality, integrity, and availability. This is an important shift, given that all too often emphasis is placed on confidentiality, when in fact a loss of availability or integrity can have a far greater impact.

Once the assets are understood and the impacts analysed, it is important to consider the threat. We have identified five areas for consideration here, but these are not exclusive, and further areas need to be identified at the local level, with equal focus applied to both internal and external threats.

As with any architectural approach, understanding the business context will help organisations understand the capabilities their technology needs to deliver, which in turn will improve user experience. Security should therefore be considered systematically, moving away from point solutions that plug holes as they appear. With such an approach, security controls become transparent to the end user and prevent the need to bypass a control due to its impact on their workflow.

In other words, security is an enabler for the business.

How can Cisco help?

Cisco's extensive security capability means we are uniquely positioned to meet your security requirements as an integral part of the network fabric, or through dedicated physical and virtual security appliances.

When developing a robust security architecture, it is helpful to think of a cyber attack as a continuum containing three main phases. Cisco has developed the simple mnemonic BDA, which represents the phases of before, during, and after an attack.

Before

This is the phase where most security investment takes place and includes the deployment of defensive capabilities such as firewalls and anti-malware. It is vital to understand that defensive controls, while important, will be breached, and so investment should be spread more evenly across the remaining phases.

During

Controls deployed in this phase focus on improved visibility, so that an attack can be rapidly identified and mitigated. Network segmentation also helps manage an attack in the 'during' phase. When implemented effectively, it can contain an attack to a limited subset of the network and IT estate.

Contents

After

The final phase of the continuum is concerned with rapid remediation. It also includes forensic controls that can help identify how an attack occurred and which systems may have been affected.

When following the BDA model, it is important to deploy capabilities that span the entire attack continuum, focusing not only on defensive technologies but also on essential elements that support rapid identification, containment, and remediation in the event of a security incident.

As the network represents the fabric of interconnectivity, it is uniquely positioned to deliver the increased visibility and control required to support rapid threat identification and containment. Technologies such as Cisco® NetFlow – a capability built into most Cisco network devices – provides real-time network telemetry revealing who is talking to whom, over what protocol, and for how long. Through careful analysis of this telemetry, unusual patterns of activity can quickly be identified and investigated. Such patterns include excessive one-way data transfer, which could be evidence of data being stolen, or data being transmitted between internal systems and Internet-based machines that are located in suspicious places.

Segmentation

Segmentation is another important capability that is delivered by the network. Its importance is always increasing, especially in light of the need to connect a wider range of devices and user communities to a common network infrastructure. Segmentation has, however, remained challenging, with many environments still relying on static segmentation, based simply upon physical location. Furthermore, the segmentation that is in place is not always used to enforce security controls, meaning that traffic is allowed to flow freely across the entire network.

The overall result of these capabilities is a system that is more responsive to threat and that can quickly identify issues as they emerge, allowing for rapid remediation and recovery, and ensuring that the organisation is able to operate unimpeded.

A top-down approach to security

Addressing the challenges covered in this paper requires a top-down approach to developing a cybersecurity strategy. Cisco Security Advisory services can support local government organisations in achieving this goal by:

- Identifying organisational risks based on analysis of the information and business impact if breach or loss were to occur

Contents

- Performing a gap analysis to identify areas of weakness between the required level of control versus the current state
- Highlighting strategic areas for security investment across the organisational, policy, and technology domains to support the secure delivery of front-line services

Digital technology has the potential to have a truly profound and highly beneficial impact on organisations across local government. However, this ever-increasing reliance on technology requires a comprehensive security architecture that is driven from the top down.

Cisco is uniquely placed to support our customers as they develop this vital capability. Contact us to find out how.

Cisco TrustSec® encompasses a range of capabilities that enable software-defined network segmentation. This is the ability to dynamically apply a segmentation policy as a user or device connects to the network, either wired or wirelessly.

Cisco TrustSec can capture details about the connected endpoint to inform policy decision making. These can range from simple user identifiers to device types, installed software and compliance with software policies (such as whether the device has the latest patches installed). By gathering this information, the system is able to make an informed decision and enforce a predefined security policy, helping ensure that the device is given the access it needs and no more. For example, this information could be used to enforce dynamic segmentation between social care and NHS staff members, so that both communities have the access they need to perform their function and limiting access to all other systems. Contact us

Cisco NetFlow and TrustSec represent just two of the many innovations that Cisco has developed to embed security into the fabric of the network. The Cisco portfolio also includes a full suite of capabilities, ranging from perimeter access control and intrusion prevention to advanced network and endpoint anti-malware solutions.

Importantly, each distinct component is able to operate in conjunction with others, forming a tightly integrated security system that can share threat and context data.

Contents

Contact us

Cisco has a dedicated team supporting our UK health and care and local government customers. The team's extensive industry knowledge means that they can identify the right Cisco solution for your needs.

Contact us for further information.

Authors

Mike Badham
Senior Solutions Architect – UK Health and Care and Local Government 020 8824 4138

Mark Jackson
Principal Information Assurance Architect – UK Public Sector 020 8824 8535

cisco.co.uk/localgovernment

C07-740499-00 05/18