A new angle on cybersecurity

New threats demand new approaches.
An expert point of view from BlackBerry Cybersecurity Consulting

BlackBerry security software

BlackBerry® software provides the embedded intelligence to secure the EoT, so that the IoT can thrive. These are just a few of the capabilities of BlackBerry software:

BlackBerry® Cybersecurity consulting solutions combine the very latest advances in endpoint security, as well as access to a constant flow of new thinking and new innovations

BlackBerry® UEM manages your diverse and growing set of devices from a single console

BlackBerry® Workspaces enables secure document sharing on any device

BlackBerry® Dynamics provides the foundation for secure enterprise mobility by offering an advanced, mature and tested container for mobile apps

BlackBerry® AtHoc™ is a complementary offering that unifies crisis communications within/between companies (including triggering organization-wide alerts in the event of cyberattacks or breaches)

Cybersecurity: bigger numbers, bigger threats

Among industry analysts and experts there is little debate that the cyber-crime wave is fast becoming a tsunami.

Predictions include the continued quadrupling of cyber-crime every 4 years with the financial cost alone reaching over $6 trillion by 2021*. Big numbers indeed and that's despite bodies like the World Economic Forum reminding us that a significant proportion of cyber-crime goes undetected – especially where industrial espionage and unauthorised access to confidential data and documents is hard to detect. Add to this the lack of clarity and law enforcement accountability associated with cross border prosecution of data breaches and the scale takes on even greater significance.

Even if you doubt the accuracy of such numbers, the conclusion is glaringly obvious: the problem's big, and it's only getting bigger.

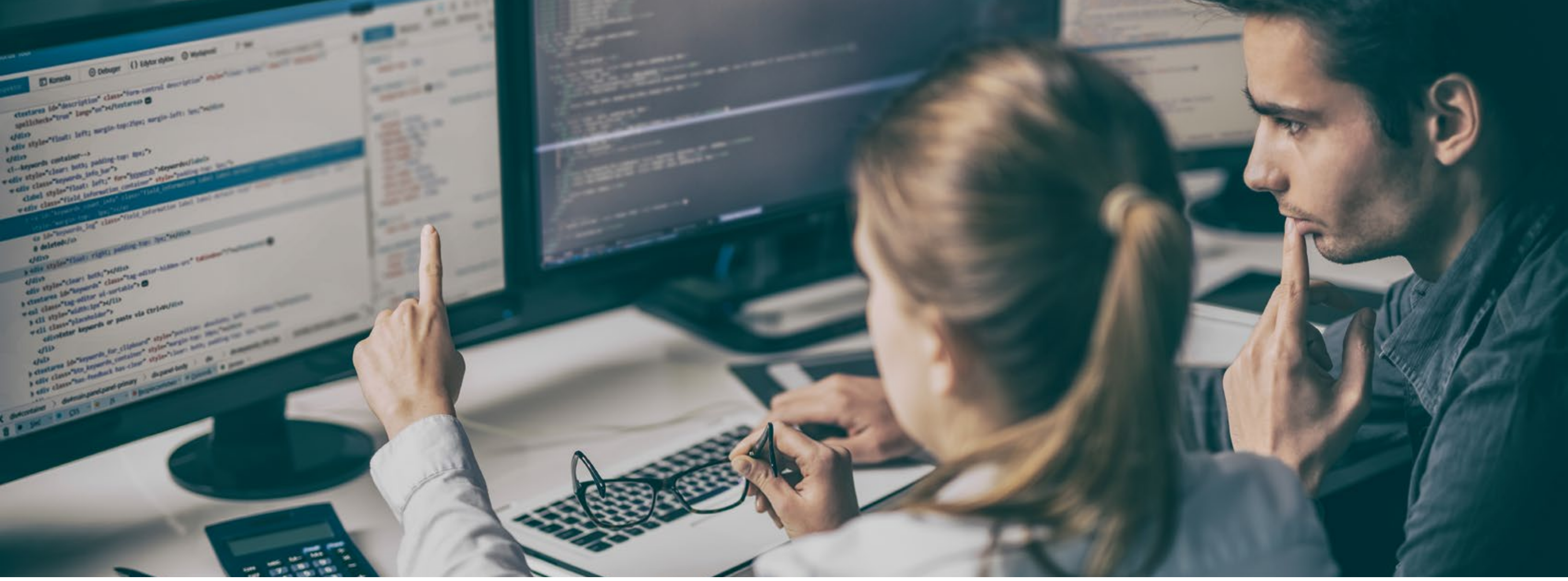
As for why this is - the most immediate factor is simply the expanded attack surface. There are predictions of an increase from 6.4 billion different endpoints to over 46 billion by 2021*. An expansion that even the increased cyber spend in cybersecurity (estimated to be approaching $1 trillion annually) is struggling to keep pace with. Compounding this is the current skills gap in IT security, with analysts predicting that the number of unfilled positions now stands at more than 3.5 million, with no short term remedy in sight*.

The forces of change

Such numbers help quantify the scale of the problem. They also help question the trust and challenge the effectiveness of established techniques for securing the enterprise. An approach typically defined as 'castle and moat', where solid, six-foot strong walls are first put in place around core on-premise resources (castle), then extended out to cover the many different access points (moat). The trouble is that such a model is not up to the task of securing a cloud-enabled world, or the multitude of Internet-enabled devices (many of which are owned by external parties), demanding access through the front gate.

As a result, castle and moat defences can contribute to a false sense of reassurance: that once inside the walls, all data and assets are safe. This view however does not connect with the reality of the threats we face today, where internal process weaknesses combined with the way people access information (and from where) can quickly compromise any static defence. Indeed, a recent survey conducted by CCS Insight** suggests that over half of all software used or managed within an organisation can now be accessed directly through a mobile app. The conclusion: effective cybersecurity today involves many separate moving parts, from different devices and endpoints, and requires fully educated employees, that need to act harmoniously to reduce both external and internal areas of exposure.

*Source: Juniper: The Internet of Things: Consumer, Industrial & Public Services 2016-2021, 2016
**Source: Security and Artificial Intelligence Shape IT Buyer Priorities in 2017, CCS Insights

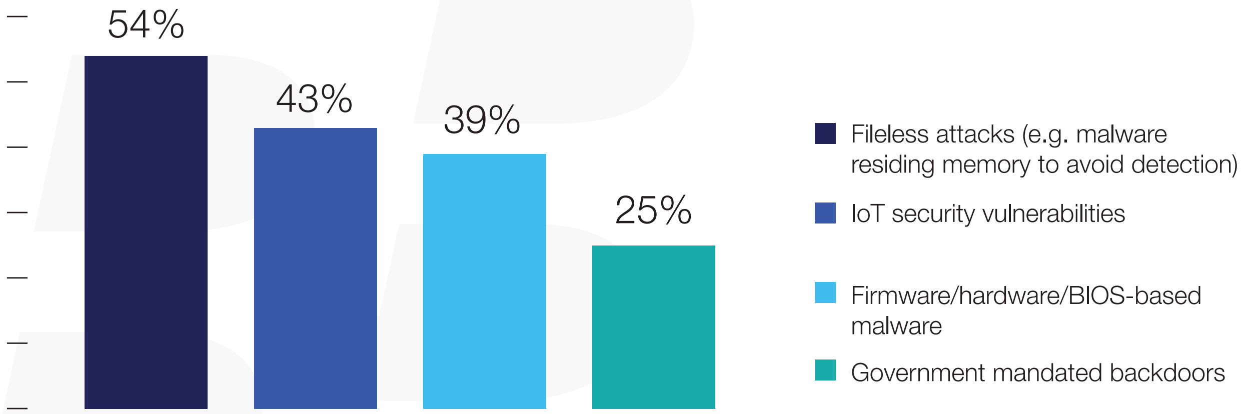


The state of play

It’s fair to say that most companies are far more up-to-date today on the risks posed by cyber-attacks than they were even two or three years ago. It’s also fair to say they’ve had no choice: ransomware in particular has demonstrated not just the ability of attackers to exploit any vulnerabilities – but also the minimal effort required to do so. It doesn’t have to be sophisticated to have a significant effect on a business. Add in the penalties with the expansion of privacy laws with GDPR, and the media’s willingness to name and shame exposed companies, and we have a scenario where all the incentives are there for attackers to increase the volume and frequency of their assaults.

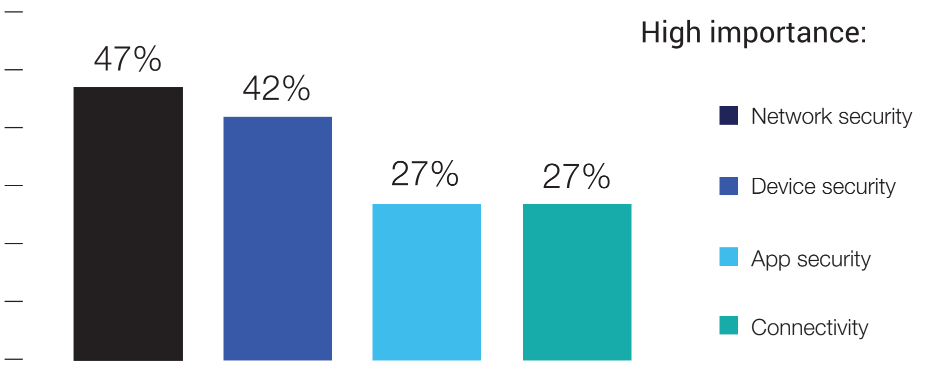
At the same time the threat landscape continues to evolve at breath-taking speed. From concerns about the security protocols in IoT devices to ‘fileless’ malware that conceals itself in memory never leaving a trace, organisations face unprecedented threats – and need to urgently move on from deciding how much to spend on their IT defences, to where to spend their budget.

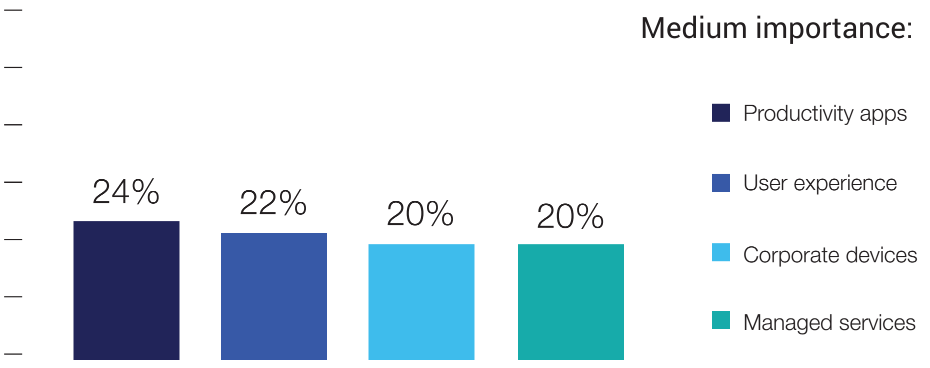
Which emerging threats are creating the most concern?*



*Source: Enterprise Security Review 2017, Computing Research

Spending wisely: enterprise budget priorities in 2018[*]


High importance:


Medium importance:

[*]Source: Security and AI Shape IT Buyer Priorities in 2017, CCS Insights

How secure is secure enough?

According to McKinsey, a good place for organisations to start when defining their security strategy is to understand their 'value at risk' equation – and then apportion resources based on the results.

Value at Risk = Impact (cost) X Threat (likely attacks) X Vulnerability (gaps in defenses)

Cost can mean different things to different organisations – with multiple types of loss extending far beyond financial. From reputational loss, the advantage a competitor may gain from an organisation's misfortune, loss in customer trust, faith and belief in a brand, reduced productivity, to the hard financial cost that is widely reported. A cybersecurity consultancy can guide organisations through this evaluation to determine how secure is secure enough.

And even while it's estimated that cyber-attacks cost billions annually, such numbers can prove a distraction. That's because even financial cost is relative: losing £2 million if your turnover is £5 billion is troubling but not a major concern; losing £100,000 to ransomware when your yearly profit margin is £1.5 million is a different problem all together.

Guiding principles

Such 'relative' thinking can also be useful in helping size potential risks, and in creating a priority list of the capabilities and processes required – and the cost of doing so.

Another cost to be considered is the cost to the business of cybersecurity in terms of people and processes. The fear of a breach can often lead to the enforcement of draconian security policies that have the collective impact of reducing business agility. Enforcing rigid access rights that prevent mobile workers from accessing the systems and apps they need to do their jobs being a good example. The need is for an adequate balance between efficiency, productivity and security.

This is a concern that touches on all aspects of the risk equation, as disenfranchised employees will typically look for ways around any obstacle. They will look to utilise unauthorised apps like Dropbox® (threat), work on files outside of the security infrastructure (vulnerability), and therefore run the risk of losing this data to an external source (impact).

Good security on the other hand helps transform employees from being the 'weakest link' to being proactive, security champions. Evolving to a scenario where business and security targets are aligned and the ultimate goal of naturally occurring business-as-usual security is achieved. This is achieved with the delivery of cybersecurity capabilities that are intelligent and flexible enough to cater for individual work practices, building on the experience from those they utilise on their own personal devices and smartphones.

Defining a new cybersecurity reference architecture

If the centuries old castle and moat inspired defences are becoming increasingly irrelevant, what's the alternative?

What we know is that securing a digital infrastructure is now less about the 'walls' of the protective barriers put in place, and more about the doors (read: access points) – and the locks that go with them.

So as the focus shifts from firewalls and infrastructure, the issue becomes the broader consideration of securing data as a whole across more endpoints, more remote users - and involving more data too.

It's a different mindset, which demands a different methodology.

One that represents a transformation in security thinking: it now makes a lot more sense to begin securing assets, processes, and communications from the edges of a business, before moving into its centre.

In other words, it's now about creating multi-layered, defence-in-depth capabilities that begin at the endpoint – before moving on to cover all users and critical infrastructure.

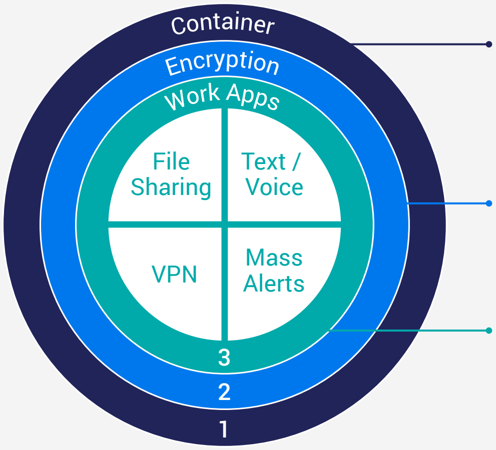
And it's here where BlackBerry's decades of cybersecurity expertise and proprietary technology can enable this new methodology to empower secure and efficient business in the new super-connected complex environment.

At BlackBerry we think differently: we start at the endpoints and deliver security from there inwards.

It's a critical difference and one that is becoming increasingly relevant – and increasingly essential.

Start at the endpoint, deliver security inwards

Three layers that deliver multiple benefits to both business users and the IT function:



Layer 1
introduces a container, embedded deeply into the hardware – a critical consideration needed to counteract the many unknown and untrusted endpoints now requiring access

Layer 2
is encryption, with its focus on risk mitigation and preventing data loss if and when an attacker gains access to core systems and apps

Layer 3
is formed by our own work apps – that shift the focus from defence to supporting key business processes in a flexible and agile manner

User benefits:

- Anytime, anywhere, any device access – to support their experience with a familiar, powerful, and trusted environment
- Business workflow optimisation – meaning they can access the data and tools needed in an easy and seamless fashion

IT benefits:

- A single policy set – that can be deployed to any endpoint at any time
- A single console – for managing all users, devices, apps, content, and communications
- Secure, military-grade encryption – for data-in-transit and data-at-rest

Keeping 'things' secure

Endpoints do of course comprise many of the 'things' in the Internet of Things (IoT): the ever-expanding number of items embedded with electronics, software, sensors, and network connectivity. A concept that's truly transformative in nature, and emerging as one of the most significant developments of our time. Not that it's just a concept: the IoT is already a reality and connecting people and 'things' together – and transforming the way they create and exchange data.

The challenge with all of this of course is that along with almost limitless potential, the IoT introduces vast new security threats and avenues of attack. An attractive target it makes too, as each 'thing' relies on the Internet for connectivity – thereby offering an indirect path to the cloud-based computing and storage resources needed to collect and analyse the data being generated. Such a network therefore demands security that can be extended to every 'thing' and every endpoint, to ensure effective protection against data loss, service theft, and denial of service attacks – in a scalable manner.

Turning IoT into the EoT

Now apply these concerns to a business, and to an organisation looking to employ connected devices to become smarter, faster, and more productive.

This is the Enterprise of Things, which is expected to grow to 19.9 billion devices by the year 2020*. Such EoT 'things' will come in many shapes and sizes; from weight sensors on trains to detect true passenger numbers, to embedded medical devices monitoring biometric data of high risk patients.

Making the EoT safe is therefore both a huge challenge and a huge opportunity, and one that BlackBerry is well-positioned to support.

In fact, we're recognised as the leading software and services company for securing the EoT. A view supported by Gartner in their recent report on 'Critical Capabilities for High-Security Mobility Management - Gartner 2017', where BlackBerry came out on top in each of the six categories - including those for government grade, commercial grade, shared data, shared devices, non-employee, and BYOD.

> "Almost every product in BlackBerry's bag of tricks directly or by extension is addressing the challenges of managing a diverse set of IoT devices."
>
> Chris Marsh, 451 Research*

*Source: BlackBerry is back: strategy and product insights point the way forward, 451 Research LLC, February 2017

Comprehensive coverage

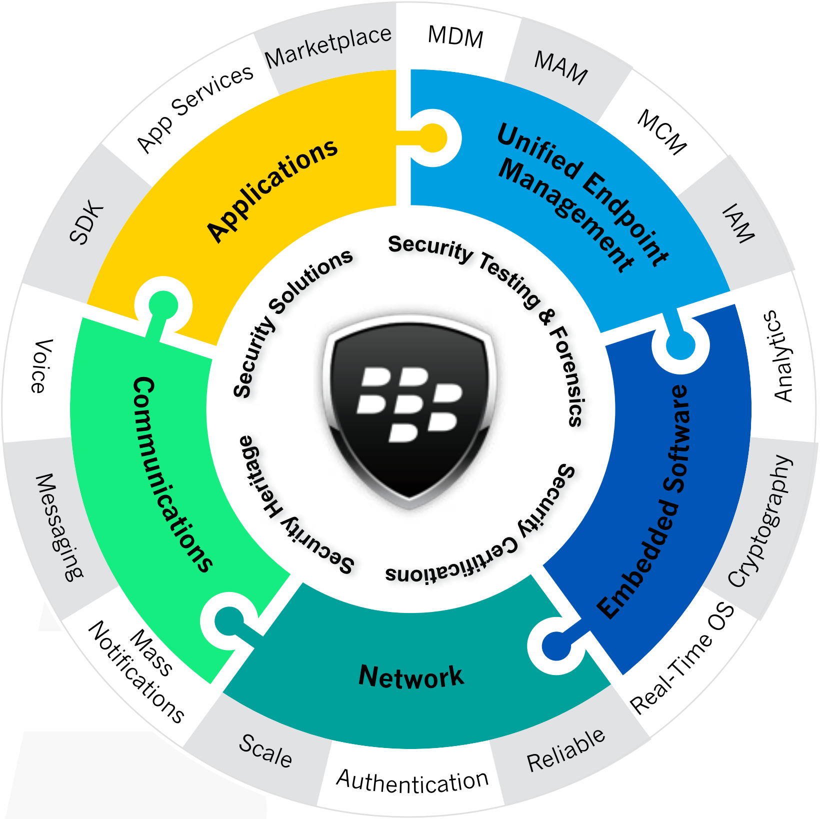
BlackBerry® Cybersecurity consulting offers a complete range of solutions that combine the very latest advances in endpoint security, as well as access to a constant flow of new thinking and new innovations.

BlackBerry® Unified Endpoint Management (UEM) a single console that offers the ability to manage all endpoints – from wearables to sensors, smart cars, and access controls.

BlackBerry® AtHoc™ to offer peace of mind through Business Continuity by effectively covering cybersecurity and employee safety over any device.

BlackBerry® Apps access our enterprise ecosystem and find nearly 4,000 custom apps that help facilitate secure collaboration, data security, and data loss prevention.

BlackBerry® Workspaces allow any file to be confidentially shared by any device, using state of the art security, enabled on an employee's own device, so policies such as BYOD can be implemented without compromising security.



BlackBerry's Global Professional Cybersecurity Services Practice

BlackBerry's consultancy practice making industry-leading threat mitigation and Cybersecurity services available to organisations requiring tailored security strategies.

Strategic Security:
Best practices in IT operation ranging across enterprise, mobility management and cloud services

Detection, Testing, and Analysis:
Threat detection, penetration testing, vulnerability and red team assessment and incident response

Automotive and IoT Security:
Connected device security consulting

Technical Security Development:
Technical assistance for infrastructure and secure product development lifecycle

In-Market Vulnerability Management:
In-market product servicing to watch and monitor product and software threat landscapes

Technical Security Training:
Cyber courses accredited by NCSC, IISP and Tiger Scheme

Thinking of getting in touch about BlackBerry solutions?

Please visit www.blackberry.co.uk

To discuss your cybersecurity challenges with a BlackBerry specialist, please visit: blackberry.com/contactsales