

# Technology

THE SECURITY ISSUE

# Leaders

## SECURITY: ARE YOU AHEAD OF THE THREAT LANDSCAPE?

### INSIDE THIS ISSUE:

#### Security to enable business

SABMiller Global CISO Mark Brown ensures risk management creates lasting success

#### The key to information security

Five key areas that should form part of the CISO's business strategy

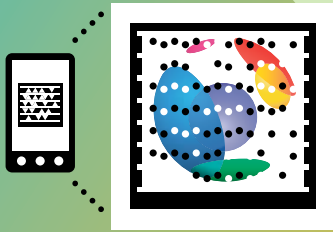
#### Education, education, education

Information Security Forum analyst Mark Chaplin says IT leaders must talk tough

#### Dealing with the cyber threat

Claire Davies MBE says businesses need a multi-layered approach to security





Want to view Technology Leaders online including previous editions? Simply download the free mobile app for your phone at <http://gettag.mobi> and then scan the tag above.

# Ahead of the chasing pack

CIOs attempting to create a tight hold on security matters face a significant range of challenges. And the scale of the problem is intensified by a confluence of economic and technological concerns.

Continuing economic uncertainty means errant individuals are likely to try and find ways to expose security loopholes for financial gain. At the same time, an ever-increasing plethora of devices and applications are being used to access and manipulate enterprise data on the go.

What was once locked down, and kept tight behind the firewall, is now open and available. And the transition means maintaining company security has never been tougher and more business critical.

## websense®

### Blended security for the social web.

**Websense is the ONLY company to offer unified web, email and data security so you can control the dynamic web.**

No visibility into social media; an inability to spot browser-based malware; no easy way to protect against data loss over collaborative networks. Sound familiar?

Websense has redefined the term 'unified' with one console managing web, email and data security. Now you can get a blended perspective on threats that span multiple vectors—the type of threats that hackers use to bypass defences.

If better security wasn't enough, Websense also lets you blend on-premise and hosted security, all managed from the same console.

Download an Acceptable Use Policy template that's relevant for companies who allow access to the social web in the work place, at [www.websense.com/aup-uk](http://www.websense.com/aup-uk)

*"TRITON Security Gateway Anywhere... Websense delivers a superb range of sophisticated web, mail and data security features that are easily managed and look unbeatable value!"* SC Magazine Review, July 2011



## CONTENTS

# 04

Mark Brown,  
Global CISO,  
SABMiller

# 06

Five key areas  
for information  
security

# 08

Mark Chaplin,  
Analyst, Information  
Security Forum

# 10

Claire Davies  
MBE, Security  
Consultant

# 11

Unlocking the  
business value  
of IT security

BT Engage IT is already committed to highlighting best practice advice for IT leaders. Our recent Showcase event in London illustrated the challenges faced by CIOs and their chief security counterparts, drawing on the knowledge and expertise of some of the UK's leading security experts.

We build on such evidence in this edition of Technology Leaders, which investigates the challenges faced by CIOs and then presents advice on the most effective ways to evaluate and manage IT security risks.

Cover star Mark Brown, Global CISO at SABMiller, is working hard to ensure his risk management style creates lasting business success. In an exclusive interview with Technology Leaders, Brown explains why IT leaders need to re-educate the technology and business community, so information management is the new lingua-franca of the security worker.

We also provide an insight into where future risks are likely to emerge, and tips on how best to tackle them when they arise. Mark Chaplin, Principal Research Analyst at the Information Security Forum, says most CIOs still have an awful lot to learn about information risk management.

And Claire Davies MBE, a former Consultant with the British Forces, suggests the online environment represents a new battle space and senior IT executives must work to help ensure the business is ready for all eventualities.

Being ready is a tough task for the CIO, especially as information security presents an ongoing – and ever-changing – game of chase. But an IT leader that makes the right preparations is likely to ensure their business is always one step ahead of its malevolent pursuers.

**John Thornhill, CEO, BT Engage IT**



You'll never know who's plotting the next cyber attack on your business. But with F5, you're protected.

Unlike traditional or so-called "next generation" firewalls, F5 security solutions identify the nature and source of digital traffic and quickly adapt to threats.

Attacks are blocked without shutting down the works. Your precious applications and data remain untouched, and your defences evolve as new threats appear.

Learn more at [f5.com/smarter](http://f5.com/smarter).



Being Chief Information Security Officer for one of the largest brewers might seem like an intractable challenge but Mark Brown, Global CISO at SABMiller, is working hard to ensure his risk management style creates lasting business success.



## Security to enable business

“I don’t think enough CISOs ask the business about its appetite for risk,” says Brown, looking back on his first two years in the role and comparing his approach to that of his IT peers. “CISOs need to re-educate the technology and business community, so information risk management is the new lingua-franca of the security worker.”

Brown speaks from a position of considerable experience. Having previously worked as a Security Manager in the IT industry, and as an Intelligence Analyst for Her Majesty’s Forces, Brown became Group CISO at SABMiller in January last year.

The brewing giant operates in 75 countries, employing more than 70,000 people. Brown has a worldwide remit to move the organisation from a traditional and reactive means of IT security to a more proactive approach, which uses technology tools and global processes at a holistic and global level.

Key priorities currently include a network and firewall simplification project, alongside BT Global Services, which allows Brown to make sure legacy technology meets the standardised demands of modern business requirements. He also pays close attention to compliance.

Rather than relying on a reactive approach to security management, Brown takes a detective and preventative attitude that is governed by a strong comprehension of business risk.

## “We’re not a regulated bank, we can take more risk – and working in emerging markets means we have to.”

“We have to be business-focused and we want to be an enabler. As a blue-chip company, our business is extremely global and we operate in a disparate range of cultures. When we look at security, we think about brand reputation and how we can make sure information isn’t leaked that might affect our market capitalisation.”

Brown says a business-enabled approach to information security management must articulate the c-suite language of risk, rather than the traditional technical idioms of IT security. Rather than relying on a series of technical point solutions to lock down access, Brown uses a series of established business processes to define how data can be exploited.

A good example comes via Brown’s approach to the management of mobility. Apple iPhones have been used across the organisation for two years and are particularly prevalent in Latin America. Not being as heavily regulated as other sectors means SABMiller has been able to think quickly about how mobile technology is used to achieve business aims.

“It’s about doing things simpler and better, and to reduce cost where possible,” says Brown, who says his team have considered carefully how mobile devices are used securely. Process-driven issues actually produce more complications than security considerations, and Brown says CIOs need to be aware that traditional legal guidelines are unlikely to be sufficient.

“Your existing policy set for acceptable use will not work in the consumer age,” he says. “The traditional IT helpdesk will not know how to manage non-Windows systems. Consumerisation has to be balanced against risk and, if you implement a buy-your-own-device strategy, you have to think about who will be responsible for areas like patch management.”

Brown takes a similar stance to the cloud, encouraging other IT leaders to see the rise of on-demand computing as a means to reset security policies and to reinvigorate the business appetite for technology. “I fundamentally believe we have a once-in-a-lifetime opportunity,” he says.

## “We must recognise the opportunity and think differently; we can help, not hinder, the business.”

Funding for IT security is traditionally justified for specific particular projects. Yet Brown says the confluence of consumerisation and the cloud means security professionals can finally use real business aims to justify the implementation of key information management systems, such as data leakage prevention, network access control and virtual platform technologies.

The message, then, is clear: justify security measures through business processes. Brown, of course, recognises that some IT leaders will have to work harder than others to justify their new approach to working. While each organisation has a particular culture of operating, the diverse global reach of some firms – including SABMiller – means CISOs must take account of regional variety and local talent.

Brown says a Global CISO cannot possibly understand all variations in rules and regulations around the globe. He encourages his peers to empower staff regionally, so employees are not just subservient to the centralised headquarters but are able to fulfill the information flow at the local level.

Further detail is provided through Brown’s own approach to information security management. His regional reports take a 12 to 18-month outlook, considering what the business aims to do next year and how that objective will be reached given the current information management strategy.

Brown overarches such discussions and takes a 24 to 36-month timeframe, where he looks to the future and works with the business to match demands for growth against the broader appetite for risk. “My job is all about translating potential information security issues for the business around culture and economics, and making those concerns manageable in a day-to-day context,” he says.

When it comes to trends during the next two to three years, Brown says organisations will continue to be challenged by a range of cyber threats and consumer-led changes. He says CISOs must think about how security adds value to the business: “It’s all about a controlled revolution and seeing problems before they happen.”

## Three top tips for IT leaders looking to manage security

1. There is no such thing as IT security – Only think of security in IT terms and you will implement a series of point solutions that fail to match business demand. A true security metric is a documentation of the impact on a business metric.
2. Think like the business – If you do not consider everything in relation to broader strategic aims, you will not be able to help the organisation meet its objectives. Talk to the c-suite and understand what they are trying to achieve.
3. Get out and feel the business – You need to understand why the organisation is doing what it is doing. A good CISO speaks to employees, always appreciating how a problem affects the front-end and the production level.

From data leakage to risk management, five key areas that CISOs must deal with as they create an information security strategy for the business.

Over half of financial services CIOs spend **30%** or more of their IT change budget on regulatory compliance.

# CISOs hold the key to information security

From malicious individuals aiming to expose your organisation's information, to senior executives who demand the CISO must work with limited funds to close every potential avenue to exposure, the role of protecting company assets has never been so challenging.

Maintaining an effective balance between risk and innovation is a tough challenge for the IT leader, especially in a modern, cost-conscious environment, where the individual spend of consumer technology is increasing at a faster rate than the CIO's technology budget.

CISOs looking to create a security strategy for the business must address five key areas - data leakage, consumerisation, cloud computing, compliance and risk - and demonstrate how the IT leader really holds the key to information integrity in the digital age.

## Data leakage and end-point security

Did you know?

The Open Security Foundation reports there have been 369 total security incidents this year, affecting as many as 126,749,634 records.

What can you do?

Data leakage simply cannot be afforded. Research from independent researcher the Ponemon Institute suggests 84% of British, French and German businesses fell victim to security breaches at least once in the past 12 months, with the cost amounting to more than €250,000 for 44% of organisations.

The Ponemon Institute suggests European business leaders must consider a more aggressive, systemic security approach. Such a strategy must work to mitigate risk and include end-to-end comprehensive protection at all points in the network.

CISOs must work with trusted partners to carefully assess their potential pain points, relating this to the risk and business drivers of the organisation. Working with an external expert might seem a strange way to deal with the pressures of internal security but a tailored and managed service will help you develop an effective business solution.

## Consumerisation and the mobile workplace

Did you know?

Consumerisation is already here and is changing how your employees interact - as much as 49% of CIOs allow their employees to complete work tasks on personal devices, according to research from CIO magazine.

What can you do?

Giving workers increased access to enterprise information through a mobile device might seem like a potential security nightmare, but it does not have to be that way. And CISOs can be the key to helping the business cope.

The demand for bring your own computing and mobile devices, that can work alongside social networking tools, means organisation must review both their short and medium-term strategies. There is still much work to be done in terms of IT strategy, with researcher IDC reporting just 4% of European IT professionals believe their organisation has modernised customer-facing applications to work with mobile devices.

Analyst Gartner suggests CIOs must build the next generation of mobile strategies to meet rising expectations from employees and customers. Such strategies should cover elements such as collaboration, multi-channel and bleeding-edge innovations, such as Near Field Communication, while still retaining security policy and posture.

# Security measures must be implemented in a controlled, yet timely manner.

## Cloud computing and the threat landscape

Did you know?

On-demand IT will quickly become mainstream, with analyst Ovum predicting that global spending on public cloud services will grow rapidly from £11.4bn in 2011 to £42bn by 2016.

What can you do?

Cloud is coming but you cannot take its evolution in the enterprise for granted. Independent research organisation Ponemon Institute suggests more than half of United States organisations are already adopting cloud services, but only 47% believe on-demand services are evaluated for security prior to deployment.

Worse still, the cloud is often being introduced beneath the radar and without the watchful eye of the CISO. Ponemon reports 50% of US IT professionals believe their organisation is unaware of all the cloud services currently deployed in the enterprise and such neglect raises the spectre of potential security risks.

The traditional security policy that concentrates on defence in depth will no longer translate to cloud computing. The CISO will be held accountable for security breaches and will need to ensure security is adequately addressed at the start of every business initiative. Security measures must be implemented in a controlled, yet timely manner, and should result in the establishment of a common risk language across the organisation.

## Compliance and regulatory concerns

Did you know?

Over half of financial services CIOs spend 30% or more of their IT change budget on regulatory compliance, according to research from consultant Xantus.

What can you do?

The ever-increasing regulatory burden is not just confined to financial CIOs and is a challenge common to IT leaders across all sectors. Research from security association ISACA suggests as much as 95% of IT professionals within major organisations consider governance to be important.

Key initiatives include Payment Card Industry standards, with analyst Gartner estimating that PCI compliance costs organisation an average of \$1.7m across a two-year survey period. Mobile and cloud computing create further governance headaches for CIOs charged with compliance management.

IT leaders must ensure the regulatory burden is fully understood. While ISACA research suggests as much as 70% of heads of IT are also a member of the senior management team, that still means almost a third of CIOs are not in a position to influence security spending decisions at the board room table.

## Risk and security hot spots

Did you know?

As much as 26% of Britain's mid-size technology companies are highly exposed to the risk presented by cyber crime according to research from insurance company Zurich.

What can you do?

A thorough understanding of risk is set to rise in prominence on the CIO agenda. Researcher IDC reports financial firms currently spend in the region of \$56bn on risk technology, a figure set to rise by 7% through 2015, driven by the increased need for compliance and a demand from the business for deeper analytical information.

CISOs aiming to deal with risk must find a careful balance between utility and innovation, while dealing with disjointed data legislation around the world and the risk of greater disruption to operations caused by infrastructure failures. CISOs must also help to drive cost savings and efficiencies within the organisation at the same time as they encounter a number of targeted threats to their organisations, such as acts of economic espionage and the work of disgruntled employees.

Rather than talking in technical terms, IT leaders must explain how failing to address a concern will lead to specific risks to the business and this explanation must be able to be related to key business performance indicators. The CISO must use risk to implement innovative IT solutions that secure the business and should be fully prepared to advise the business on the cost of not implementing such solutions.

The Open Security Foundation reports there have been 369 total security incidents this year, affecting as many as 126,749,634 records.

When it comes to information security and risk management, the end of term report for most CIOs is pretty conclusive: could do better.

The description comes from Mark Chaplin, Principal Research Analyst at the Information Security Forum (ISF), an independent association representing many of the world's leading firms. Chaplin helps the organisation produce a series of reports and standards, and is an expert in educating IT leaders about how to deal with the ever-changing threat environment.

His research leads him to suggest that most CIOs still have an awful lot to learn about information risk management. The need for such awareness becomes even more acute in a modern era of technological development, which means businesses must balance the opportunities of collaborative operations against the risks of cyber terrorism.

# Educating the business about information risk

**“This is a fast changing world, where business objectives move dynamically alongside strategies and technologies, producing new expectations inside and outside the organisation.”**

**Mark Chaplin**  
Principal Research Analyst

"I don't think any executive can be totally ready for the range of information security threats," he says. "This is a fast changing-world, where business objectives move dynamically alongside strategies and technologies, producing new expectations inside and outside the organisation."

## How can CIOs become information experts?

CIOs, says Chaplin, have traditionally been concerned with the management of technology. The technical-based emphasis of the role is reducing, such that the more effective IT leaders are now responsible for the value of organisational information.

"There are CIOs who are working effectively with the business to produce successful information management strategies at the boardroom level," says Chaplin. "These leaders have the ear of the chief executive and they truly understand the significance of information risk."

He argues an awareness of risk is absolutely fundamental for the modern CIO. Other c-suite executives have an understanding of risk and can articulate the need to make crucial business decisions, sometimes without a lack of clear information.

"Some threats are on the radar and require the CIO to deal with risks on a daily basis," explains Chaplin. "Other risks are below the radar and more difficult to deal with, and some are black swans that could have a catastrophic effect."

He points to the Japanese earthquake in March 2011 and related concerns at the stricken Fukushima nuclear plant. The combined effects on society and economy, including supply chain processes, became manifest as a cluster threat, where a number of circumstances came together with appalling and completely unforeseen consequences.

Risk must be placed within the wider business context, where the potential impact of an information and security threat is understood only in relation to wider financial, operational and customer service concerns. CIOs need to explain how much loss the business, in the event of a low or high impact event, can be expected to shoulder.

So, for example, would the loss of a network in part of Southeast Asia be catastrophic at a global business level? A CIO that is able to communicate the risk in terms the business can quickly comprehend is in a great position.

"That's a powerful statement," says Chaplin, who urges IT leaders to avoid thinking of IT security in purely point-based solution terms and to instead empower fellow executives with useful business information. "Understand what your audience wants and recognise that, when it comes to reporting the facts, different areas of the business need specific types of knowledge."

## What should IT leaders do next?

Chaplin believes context is also absolutely crucial to understanding the current "hot buttons" within the technology industry, such as consumer IT and cloud computing. Such trends will continue to affect the organisation but Chaplin urges CIOs to not get too over-involved in the vendor hype.

"Don't cry wolf to the business," he says.

**"Think about how you can add value as you start to think about the future of your organisation's operations. As you think about the future, you will need some sort of model to help guide your thinking."**

The ISF addresses such concerns through its annual Threat Horizon report. Starting in 2006, the research identifies the key areas of risk to business, both within and beyond the information security remit. Chaplin says key themes CIOs will need to address during the next two years include protectionism, breach identification and mobile technology.

"Consumerisation is here, yet debates continue about the potential risk," he says. "Some CIOs are embracing the trend and others are relying on an avoidance strategy. But consumerisation is going to impact your business whether you like it or not. You simply must prepare."

Chaplin says: "IT leaders should again analyse the threats and opportunities associated to themes, like consumerisation and the cloud, within the wider context of business operations. Don't be too reactive and get too caught up in the marketing bluster."

"Be proactive, go to the board and explain what on-demand technology means in business terms. Make sure you have the information to explain why the cloud is nothing to worry about."

## Five top tips for dealing with information risk management

1. Controls can be difficult to justify in a modern and flexible business environment, which presents a challenge for CIOs. Take a risk-based approach, rather than a compliance-based approach to information security, which explains the potential cost of loss to the business.
2. Weave good practice into your daily activities. Look inside out at your organisation and think about manageable and non-manageable risks. Operationally, for example, consider how your organisation relies on spreadsheets to make business decisions.
3. Think about how your fellow executives are looking at the future in their attempts to define a broader business strategy. If you start thinking about the organisation's technological and environment profile, consider such elements in relation to wider operational aspects.
4. Engage with the business at all times. Start a dialogue and create an instant management capability that allows you to flexibly deal with changing circumstances. Build such conversations on standardised themes that will allow you to explain the business threat.
5. Change your thinking by networking with your peers and gaining intelligence for the business. Become a super connector that brings people together, then build a model that addresses the security threat in your own organisation.

## Few people know more about the potential challenges a business can encounter with regards to the fast-emerging technologies used to exploit weaknesses in security defences than Claire Davies MBE.

As a former Security Consultant with the British Forces, Davies has operated as a senior investigator and boasts a hugely impressive strategic background in intelligence management. Such experience gives her a clear awareness of security concerns and she has strong advice for CIOs aiming to deal with the online threat environment.

### “Cyber security is a significant concern.”

“It reaches across borders, is anonymous and the technology that underpins the threat continues to develop. There is a huge need for business executives to understand security and CIOs must create an intelligence-led approach.”

Davies suggests the online threat represents a fifth battle space in regards to incident management. Traditional warfare took place on land, before moving to the sea and the skies. Intercontinental satellites controlling missiles provided the context for a fourth generation set in space.

The current battle space is cyber in nature and involves the heightened risk of terrorism via electronic and online means, says Davies: “The fifth generation represents something different, because portions of cyberspace can be turned on and off cheaply and quickly,” she says. “The physical barriers to entry are very low and there are threats from all potential angles.”

Such angles cover a broad spectrum of threats, from kiddie scripters working covertly in their bedrooms, to organised gangs of cyber criminals operating across national borders and on to anti-competitive practices where organisations steal rival firms blue prints. The acts themselves are often politically motivated and are becoming increasingly sophisticated.

High profile examples of cyber threats continue to make the news, including hacker collective Anonymous distributed denial of service attack on Sony and suggestions that the FBI is investigating claims that hackers in China have breached the email accounts of American officials.

Davies says: “The onus is on senior IT executives to help ensure the business is as ready as it can be. As the cyber threat increases, security professionals need to be intimately aware of the risk to business intelligence,” she says. “You might not know the specific details, but you’ll be better prepared if you act as if the security threat is coming.”

Complacency is simply not an option, due to the confluence of rising bandwidth and the year-on-year rise in digital information. A large amount of effort seems to be concentrated on preventing the type of data being stolen that could have considerable financial implications.

But addressing the legal consequences of information loss is also crucial, particularly with regards to the possible breaching of the Data Protection Act. And IT leaders, says Davies, must additionally consider the potential ramifications of a data breach upon the external reputation of the wider organisation.

“Maintaining integrity is absolutely crucial,” she says, referring to her work with the British Forces and possible models that CIOs can use to develop an intelligence-led security cycle. The cycle draws on a step-by-step approach to the refinement and development of information security and should include core elements, such as education programmes, regular meetings with internal customers, issue detection methods and security protection techniques.

Davies says: “CIOs and their security colleagues must carefully investigate particular threats, exploit information emerging from such analysis and then work to create a strategy that helps the business deal with the ever-changing threat environment.”

### “The more mechanisms you put in place, the more tools a hacker will require in any attempts to circumnavigate your defences.”

“Your security approach must be multi-layered and diverse, and the secure systems you put in place must be simple and easy enough for those across the organisation to understand but complex enough to deter even the most determined perpetrator.”

# How can CIOs deal with the cyber threat?

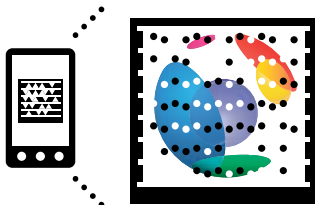


# Unlocking the business value of IT security

**A successful Chief Information Security Officer (CISO) understands that business risk, and the business attitude to risk, are key drivers for a strong IT security strategy. A strategy that can balance acceptable risk, measured in terms of real business impact, while responding to business needs across a 24 or even 36-month outlook is a true value-add; implemented in the field and recognised in the boardroom.**

**JUNIPER**  
NETWORKS

**“Juniper’s integrated portfolio of software and appliances combine to create an end-to-end cloud security architecture.”**



Find out how Juniper and BT Engage IT can help your organisation. Simply scan the tag above: [www.btengageit.com/juniper](http://www.btengageit.com/juniper)

Today, there are two major trends confronting the CISO: consumerisation of IT and the advent of cloud services. These two trends feed each other in a positive feedback spiral, with the explosion of mobile bring your own device (BYOD) users consuming ever more cloud-based services that span consumer and business applications.

The challenge, therefore, is to understand the business risks in comparison to the potential benefits of such trends in order to reach a desired balance. And a fundamental outcome of risk management is the IT security strategy.

The business opportunities of consumerisation and cloud are well documented, if not well understood. Cloud-based service delivery presumes a pay as you go (PAYG) charging structure that gives access to elastic compute and storage resource that is either hosted within the private enterprise domain, the public domain or is a mixture of both, known as hybrid.

The BYOD phenomenon makes use of the IT-savvy workforce and increases productivity through immediate and effective access to services. The combination of consumerisation and cloud allows previously unattainable levels of business agility. Users now have instant access to a rich mix of social and business applications, independent of the storage and processing power of the end device, and from any device in any location.

However, the combination of increased mobility of the user, un-managed devices and the virtualised data centre - from which cloud services are delivered - leads to a number of security challenges not previously experienced by the enterprise or service provider.

At the highest level, there is a need to deliver clean clouds, which can be understood as an attack-free zone to host and provide services in both the public and private domains. The next step of the challenge is to ensure that the largely un-managed devices accessing on-demand services are infection-free and can connect securely, without compromising data in transit.

Juniper Networks delivers innovative network security technology that underpins clean clouds. Juniper’s integrated portfolio of software and appliances combine to create an end-to-end cloud security architecture. The architecture is built on the premise of simplifying the delivery of secure cloud services, establishing attack-free zones within the virtualised data centre and ensuring the secure connection - and infection-free status - of mobile and fixed devices.

**CISOs should look for a number of key elements in a cloud security architecture:**

- An open and scalable architecture that will enable your business to adapt continuously to evolving security threats and to the needs of your business, in line with your risk management strategy.
- Integrated physical and virtual security capabilities within the virtualised data centre to enable consistent and easily deployed security policy enforcement across the physical and dynamic virtual domains.
- Visibility and insight to support proactive risk management and rapid threat response in a dynamic environment.
- Automated and simplified processes to mitigate human error, both in terms of design and operational concerns, and minimise time to react.
- Mobile device security, access and management functions that can be deployed through a simple app store to the user device for ease of deployment, integration and adoption, and which can be operating system-agnostic in support of BYOD policies.
- The ability to deploy standards-based and federated access security across the enterprise and service provider boundary to support hybrid cloud deployments under CISO policy control.

**If you are eager to unlock the value of IT security - in the cloud, on the move, anywhere - for your business, you should be talking to Juniper Networks. You can find out more at: [www.btengageit.com/juniper](http://www.btengageit.com/juniper)**

# Taming Web 2.0

How to **loosen control** without **losing control**

**Check Point Application Control Software Blade** can help you prevent risks related to the use of Internet Applications by leveraging **AppWiki**, the industry's largest library of over **50,000 widgets and apps**.



**DETECT and CONTROL**  
applications



**EDUCATE**  
users



**ENFORCE**  
data policies



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

<http://appwiki.checkpoint.com>