

The Top 5 Threats to Enterprise File Security

And How You Can Protect Your Organization



BlackBerry
Workspaces

File Security Threats

Threats to file security – both external and internal – are a growing issue. BlackBerry® Workspaces can help address these threats by securing sensitive files so that they're always under your control.

With cyber attacks ravaging the networks of governments and corporations, enterprise IT and security professionals need to adjust their data protection strategies. But in so doing, they must not neglect the threat represented by internal actors, either. This paper takes a deeper look at the file security threats – both internal and external – facing modern businesses, and how a secure collaboration solution can help you guard against them.

Specifically, it covers:

- How the recent wave of data breaches occurred, and how they impacted the targeted organizations
- How a secure collaboration solution can help improve your file security
- Key considerations for protecting data on file shares, endpoints, and collaboration systems
- Why Workspaces is the ideal solution for your enterprise

BlackBerry® Workspaces can help protect your enterprise from threats such as external hacks and internal leaks. Whether you need to enable personal productivity, facilitate team collaboration, or mobilize and transform your entire business, BlackBerry Workspaces is the best choice for secure file collaboration.

Top Five Security Threats to Your Files:

1. Extortion
2. Political motives
3. Foreign state actors
4. Loss or theft of devices
5. Internal leaks

A Brief History of File Security Threats

You may remember the 2015 Anthem data breach that put as many as 80 million current and former customers' personal information into the hands of cybercriminals.ⁱ Or you may recall the 2014 Sony Pictures Entertainment hack that put thousands of employees at dire risk of identity theft, not to mention unpublished scripts, marketing plans, and more.ⁱⁱ Or more recently, you may have heard about the 2016 Uber breach that compromised the information of 57 million riders and drivers.ⁱⁱⁱ

In the past, large data breaches were rare. However, as businesses began to store sensitive information such as customer personal information and intellectual property on corporate devices, cloud servers, online databases, and more, the chance of files falling into the wrong hands increased exponentially. Modern breaches now have a much larger impact compared to the 90's, potentially putting the information of millions at risk.

In recent years, lawmakers and businesses alike have taken various measures to keep critical data safe.

Regulations such as HIPAA, GDPR, and the PCI Data Security Standard hold businesses to strict standards where customer data is concerned. File sharing sites and content collaboration platforms provide businesses with a means of keeping workers connected and productive. However, regulations do not definitively stop data breaches from happening – and not all file sharing tools are created equal from a security standpoint.

For security-minded organizations of all types and sizes, an enterprise-grade, an IT-controlled collaboration platform is a must – and not just because of the evidence presented by history.

Major File Security Breaches

The Shmoon attack steals files, deletes them locally, and disables hard drives on 30,000+ workstations at Aramoc.^{iv}

As part of the SWIFT banking hack, malware deletes database records and alters confirmation documents to conceal the activities of hackers.^{vi}

Anthem becomes the first major healthcare provider to fall victim to a major hack, with over 80 million records compromised.^{vii}

Thousands of HIPAA-protected medical records are exposed in a data breach due to a misconfigured Rsync backup server hosted by a third party, iHealth.^x

A hard drive containing the personal information of approximately one million people is stolen from a Washington State University storage unit.^{xi}

Hackers choose HBO's Game of Thrones as their target, pilfering everything from sensitive internal documents to two episodes of the show, which they leak early after the company refuses to pay a several-million-dollar ransom.^{xiv}

An unemployed man finds a lost USB stick containing several hundred critical documents related to security at London's Heathrow Airport, including protection plans for the Queen and visiting foreign dignitaries.^{xvi}

2012

A hacker group known as "The Guardians of Peace" attacks file shares and workstations at Sony Pictures. The attack is later attributed to the North Korean government.^v

2014

The "Panama Papers" has been called the largest data breach in history. 11.5 million documents are stolen by unnamed hackers from Panama law firm Mossack Fonseca and released to the public.^{viii}

2015

2016

Premier Healthcare reports a data breach after a laptop computer was stolen from their headquarters. The laptop was protected by a password, but its files were not encrypted and contained healthcare data of over 200,000 patients.^{ix}

2017

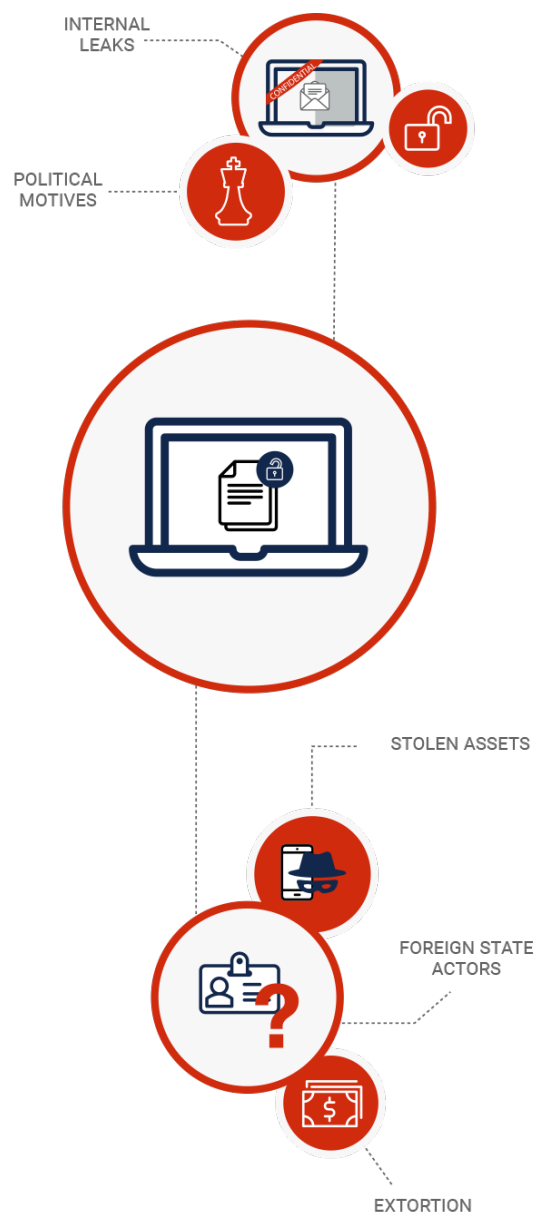
A massive attack, the WannaCry infects millions of computers, impacting more than 200,000 businesses in over 150 countries.^{xii}

A hacker with the handle 'thedarkoverlord' leaks episodes of "Orange is the New Black" and demands a ransom not to release them.^{xiii}

Equifax suffers a cyber attack that impacts at least 143 million consumers, a recent breach that had a large scale impact.^{xv}

Uber reveals that in 2016 it suffered a breach that exposed the personal information of 57 million Uber users and drivers, but chose to pay the hackers \$100,000 to keep the breach under wraps. The data was accessed by hackers after password information was erroneously stored on GitHub.^{xviii}

Knowing Is Half the Battle – Understanding the Threats Facing Your Files



Extortion

Historically, hackers tended to mostly go where the money was – healthcare, financial services, large enterprises, etc. However, any business with mission-critical documents can fall victim to an extortive attack. And such attacks are becoming ever more sophisticated and targeted at new points along the supply chain.

Netflix is a prime example. In May 2017, a hacker with the handle 'thedarkoverlord' leaked the entire fifth season of "Orange is the New Black" by infiltrating a post-production company used by several major movie studios.^{xviii} Once the hacker broke into that company's servers, they downloaded an unknown quantity of movies and shows, demanding a ransom not to release them.

It doesn't matter how much a business strengthens its own security if they lose control of critical files in the hands of its partners or vendors. There is no way to guarantee a partner or service provider will treat critical data with at least the same care as that data's owner. And the more external agencies and contractors a business works with, the greater the risk of losing control of critical files.

By storing intellectual property and other critical data in a secure, encrypted repository, an organization increases its protection against ransomware and other extortion attempts, whether in media, healthcare, or otherwise. A hacker cannot extort an encrypted data blob, after all. And that's true regardless of whether they attack an enterprise organization or one of its partners.

Netflix, ABC Hacker Promises More Leaks: "Hollywood Is Under Attack"

12:50 PM PDT 6/6/2017 by Tadana Siegel



Victor Keriow



A Political Statement

Not every attack is financially-motivated – hackers could also target your files for political reasons. Consider the Panama Papers leak mentioned above: 11.5 million files, including emails, invoices, and bank records.^{xix} Although the purpose of the leak was to unveil corruption amongst government officials and celebrities, many legitimate businesses and innocent individuals were also impacted.

The Panama law firm which had its data stolen, Mossack Fonseca, was specialized in helping clients establish offshore financial holdings. Unfortunately, when storing client data, it lacked basic network security such as server-side document encryption and user access controls. This left the firm vulnerable to a run of the mill spear phishing attack – and caused one of the largest breaches in history.

There were many things Mossack Fonseca could have done differently, chief of which was proper logging and access controls. Had the firm been using a secure collaboration solution, administrators would have been aware the moment an unauthorized party accessed their server (if they could even gain access at all). They could have rescinded access to those files immediately.

Protecting your business from security breaches is important, but many solutions have limited ability to limit the damage once a breach has occurred. File-level security that travels with a file – even if it has been stolen – provides that extra layer of security. If a legitimate account is compromised by bad actors, your security team can detect and mitigate the issue quickly.

They will have knowledge of which files were accessed, what was done with those files, what device they were accessed on, and even where they were accessed from. More importantly, an effective file security solution will allow IT to immediately rescind access to compromised files before they can be used for ill. Critical data is protected no matter where it is (or who's accessing it).

Sponsored by a Foreign State

Sony Pictures suffered a cyber attack in November 2014 that took down computers and landline phones during Thanksgiving week, causing an interruption in the distribution of the movie "The Interview".^{xx} After evaluating the software, techniques, and network sources used in the hack, intelligence officials suggested the attack was state-sponsored. Allegedly acting on behalf of the North Korean Government, a hacker group identifying itself as "Guardians of Peace (GOP)" leaked a large volume of data from Sony Pictures.



This data included personal information about Sony's employees and their families, information about executive salaries, copies of then-unreleased Sony films, and more. Researchers eventually identified the malware used in this attack as BKDR_WIPALL. Based on destructive malware that deletes files and causes other damage to systems and networks, the code used in this attack had a secondary purpose – data exfiltration. This continues a significant trend in external hacking attacks - malware can be designed to destroy the systems it infects, but increasingly, it is being used to steal data, information, and files.

Again, with a secure collaboration platform, a business can help protect against this type of attack, as it prevents files from being overwritten by unauthorized parties because secure file systems have access controls to prevent unauthorized users from accessing or changing the files. Properly architected, such a solution cannot be used as an entry point for malicious software. When paired with an off-the-shelf backup and recovery system, it provides an effective defense against malicious intrusion.

In short, to increase the protection of your business data, you need to consider file-centric protections in addition to shoring up your perimeter, because your files are what criminals are going to target.



Lost or Theft of Physical Assets

Data breaches are frequently caused by digital attacks – but not always. A stolen laptop or a misplaced USB stick can cause just as much trouble as a server whose security has been cracked. And unless a business already has measures in place to prevent theft, all it can do is contact the police and wait.

With a secure content collaboration platform, this becomes a non-issue. Files are protected at all times and in all locations with strong encryption on an individual basis. Access to those files can be revoked at any time or set to expire at a certain time automatically.

An equally important goal after a data breach involving lost or stolen hardware is to get up and running again as soon as possible. Making sure that files are not only protected but stored in a remote location that is accessible from multiple end-points – laptop, mobile, browser – is the key to making sure that the loss of a piece of equipment doesn't bring your business to a standstill.

Internal Leaks: The Human Element

In 2016, a staff benefits vendor working for Google accidentally emailed the names, social security numbers, and personal data of an undisclosed number of Google employees to the wrong recipient.^{xxi} More recently, in November 2017, an unlocked and unencrypted USB drive containing security data related to Heathrow Airport was discovered on the side of the road.^{xxii} Among the information on this drive were protective measures for the Queen and visiting dignitaries. Despite the best security technology and processes, history shows that security breaches continue to happen due to user error or trusted users with malicious intent.

Unless the files accessed within your organization are protected by default, your employees can share them with anyone. And this is not simply a matter of carelessness. Disgruntled staff can easily send your most critical documents to a competitor or criminal.

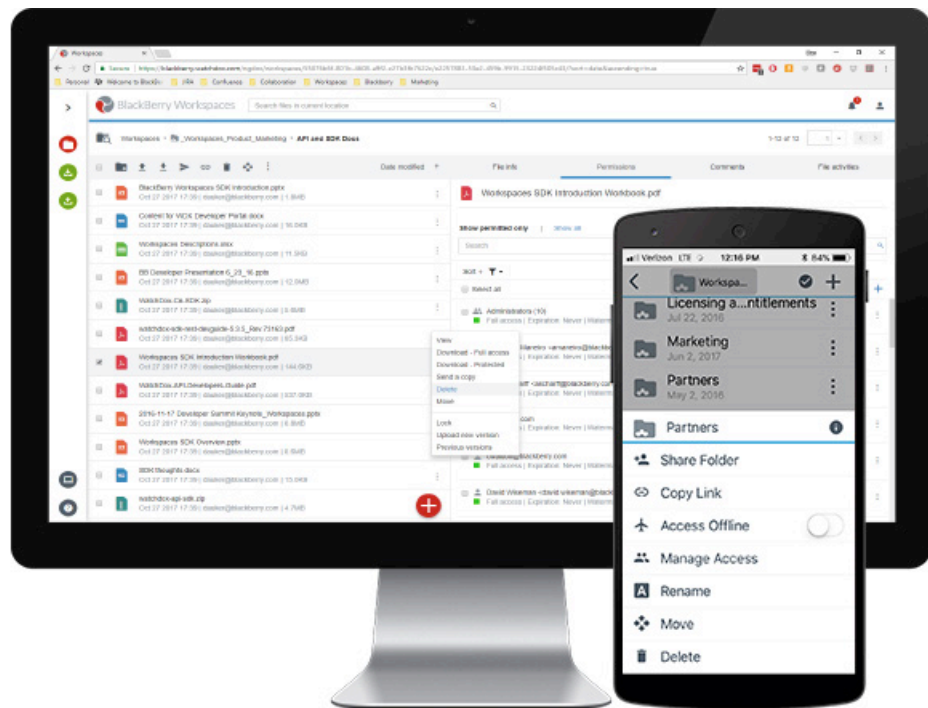
To protect your files, you need to apply encryption and DRM to them by default, even when they're being shared among employees. But this needs to be accomplished without creating an inconvenience for staff, lest they simply circumvent your security. Not every collaboration tool can surmount this challenge.



How BlackBerry Workspaces Can Help

Network-level isn't enough to protect corporate information from prying eyes. To help prevent both internal employees and external vendors from putting your data into the wrong hands, you need a secure file share solution.

That's where BlackBerry Workspaces comes in.





What makes BlackBerry Workspaces® different is its file-level security model.

Workspaces offers 256-bit file encryption and access controls to ensure that only authorized users can access your files – even after they leave your network.

Companies need a secure content collaboration platform that allows them to share confidential information with colleagues and partners, enable mobile productivity for remote employees, and securely transfer large files, all while protecting their sensitive business information.

Unlike consumer apps, Workspaces was built from the ground up to meet the needs of the enterprise. We know that document security is your number one concern, which is why it's at the heart of BlackBerry Workspaces. Our enterprise file sync and share (EFSS) platform has been recognized as a leader in multiple analyst reports, including Gartner's Critical Capabilities for Content Collaboration Platforms^{xxiii} and Forrester's EFSS Wave.^{xxiv}

The reason for all this recognition is tied to BlackBerry Workspaces' unique file-centric digital rights management technology, coupled with file-level security. Workspaces offers the following critical features:

Best-In-Class Data Security

BlackBerry Workspaces embeds digital rights management (DRM) protection in your files, so your content stays secure everywhere it goes, and you can control users' ability to view, edit, copy, print, download, or forward files, even after those files are downloaded or shared with third parties. With BlackBerry Workspaces, your employees can safely share documents, grant access to authorized users only, and revoke access anytime if required.

This access can also be set to expire after a set timeframe.

Workspaces provides file-level security combined with a user experience that's as easy and intuitive as any consumer solution. It's also the only solution that encrypts files not just at rest or in transit, but also while they're in use (via AES-256 where available, using FIPS140-2 certified cryptographic library), reducing the risk of a breach or loss of data and information.

File Synchronization and Sharing

Workspaces can help your employees work on files in the way that's the most convenient at any given time. Workspaces provides a suite of integrated collaboration tools that allow you to view, search for, annotate, edit, and share Office, PDF, and image files using your mobile device – or do it all using the native apps on your desktop.

Custom watermarks splash a user's email or IP address across a document or in the viewer to deter leaks and increase accountability. Users can also obtain legally binding signatures via a DocuSign integration. To further safeguard your files while boosting productivity, file locking allows teams to prevent duplication of effort by temporally limiting access to a document while it's being edited.

Finally, spotlight viewer blurs the screen everywhere except around the mouse cursor, further deterring those who might attempt to 'capture' the screen displaying a document.





Productivity-First Mobility

At BlackBerry, we believe that extreme, complex security measures typically hinder productivity and prevent sharing across organized boundaries and devices. But we also believe that an EFSS platform needs to do more than account for convenience – it must enable it, especially on mobile devices.

That's why BlackBerry Workspaces includes many features designed to allow employees to work anytime, anywhere. Chief among these is the ability to add annotations to a shared document – a preferred method of collaboration for mobile, where smaller screens make direct editing cumbersome.

Other key collaborative features include a DRM-protected offline mode, easy creation and management of workspaces, automatic sync across workspaces, a user-friendly, intuitive interface, and compatibility with systems such as email.

Multiple Authentication Options

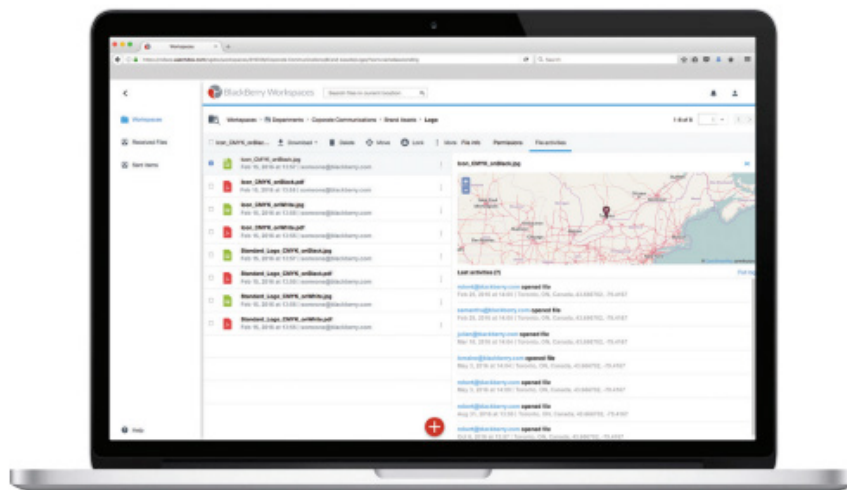
Workspaces offers multiple authentication options, allowing different types of users to authenticate in different ways – what we call multi-modal authentication. Internal employees, for example, can use their Microsoft Active Directory credentials to sign in. For external users, BlackBerry Workspaces integrates easily with OAuth and SAML and supports self-provisioning via a username and password.

File Tracking and Auditing

You can also choose to deploy Workspaces in the way that best suits your IT environment: cloud, on-premise, or as a hybrid solution. Comprehensive tracking of all document activities provides critical information for audit, compliance, and business intelligence.

And to ensure that secure data exchange doesn't create more work for IT, Workspaces provides default, a self-provisioning authentication solutions and a unique feature known as mixed-mode authentication, which allows different types of users to authenticate in different ways.

With file-level encryption, user access controls, and digital rights management protection, BlackBerry Workspaces is the solution your company needs.



Integration with Existing Architecture

You need not toss aside your existing investments to deploy Workspaces. Convenient to use for both employees and administrators, it readily integrates with existing repositories through tools like SharePoint Protector. If you already have your own infrastructure in place, Workspaces allows you to layer on security, mobility and productivity while leaving your existing architecture in place. You don't need to migrate any files – Workspaces protects them in place.



Conclusion

While there are many excellent consumer file-sharing tools on the market, they aren't like BlackBerry Workspaces. BlackBerry Workspaces is built for security, with out-of-the-box functionality ready to configure and use. When you're looking to enable truly secure collaboration within your business, BlackBerry Workspaces is the best choice.

After all, if there is one thing organizations like Evides and QIC know, it's that there's a difference between being secure and being BlackBerry® Secure™ – they chose the latter, and so should you.

For more information about these and other Workspaces customer case studies, please visit: <https://us.blackberry.com/enterprise/customer-success>



About Workspaces

BlackBerry® Workspaces makes your content secure wherever it travels. With BlackBerry Workspaces, stakeholders can safely access, share and collaborate on even the most sensitive files, using any device – desktop (Windows®, Mac®) or mobile (iOS®, Android™, BlackBerry® 10). By combining a user experience that's as easy and intuitive as any consumer solution with a unique data-centric architecture (which embeds protection right in your files), BlackBerry Workspaces is designed to meet the needs of your organization, IT team, and users.

For more information, visit www.blackberry.com/workspaces

Sources

- ⁱMcNeal, Gregory S. "Health Insurer Anthem Struck By Massive Data Breach." Forbes. February 05, 2015. Accessed January 10, 2018. <https://www.forbes.com/sites/gregorymcneal/2015/02/04/massive-data-breach-at-health-insurer-anthem-reveals-social-security-numbers-and-more/#17d70a7c2601>.
- ⁱⁱPeterson, Andrea. "The Sony Pictures hack, explained." The Washington Post. December 18, 2014. Accessed January 10, 2018. https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.6cc181e84989.
- ⁱⁱⁱMenn, Joseph and Dustin Volz. "Exclusive: Uber paid 20-year-old Florida man to keep data breach secret." Reuters. December 07, 2017. Accessed January 10, 2018. <https://www.reuters.com/article/us-uber-cyber-payment-exclusive/exclusive-uber-paid-20-year-old-florida-man-to-keep-data-breach-secret-sources-idUSKBN1E101C>.
- ^{iv}Perloth, Nicole. "Cyberattack on Saudi Oil Firm Disquiets U.S." The New York Times. October 23, 2012. Accessed January 10, 2018. <http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html>.
- ^vPeterson, Andrea.
- ^{vi}Bergin, Tom and Nathan Layne. "Special Report: Cyber thieves exploit banks' faith in SWIFT transfer n." Reuters. May 20, 2016. Accessed January 10, 2018. <https://www.reuters.com/article/us-cyber-heist-swift-specialreport/special-report-cyber-thieves-exploit-banks-faith-in-swift-transfer-network-idUSKCN0YB0DD>.
- ^{vii}McNeal, Gregory S.
- ^{viii}Burgess, Matt and James Temperton. "The security flaws at the heart of the Panama Papers." WIRED. October 04, 2017. Accessed January 10, 2018. <http://www.wired.co.uk/article/panama-papers-mossack-fonseca-website-security-problems>.
- ^{ix}Snell, Elizabeth. "Top 5 Healthcare Data Breaches in 2016 Not From Hacking." HealthITSecurity. July 08, 2016. Accessed January 10, 2018. <https://healthitsecurity.com/news/top-5-healthcare-data-breaches-in-2016-not-from-hacking>.
- ^xO'Hara, Mary Emily. "Thousands of Patient Records Leaked in New York Hospital Data Breach." NBCNews.com May 10, 2017. Accessed January 10, 2018. <https://www.nbcnews.com/news/us-news/thousands-patient-records-leaked-hospital-data-breach-n756981>.
- ^{xi}Long, Katherine. "Did you get the letter? WSU sends warning to 1 million people after hard drive with personal info is stolen." The Seattle Times. June 22, 2017. Accessed January 10, 2018. <https://www.seattletimes.com/seattle-news/education/did-you-get-letter-wsu-sends-warning-to-1-million-people-after-hard-drive-with-personal-info-is-stolen/>.
- ^{xii}"Cyber-attack: Europol says it was unprecedented in scale." BBC News. May 13, 2017. Accessed January 10, 2018. <http://www.bbc.com/news/world-europe-39907965>.
- ^{xiii}Perloth, Nicole and Matthew Haag. "Hacker Leaks Episodes From Netflix Show and Threatens Other Networks." The New York Times. April 29, 2017. Accessed January 10, 2018. <https://www.nytimes.com/2017/04/29/business/media/netflix-hack-orange-is-the-new-black.html>.
- ^{xiv}Barrett, Brian. "Breaking Down HBO's Brutal Month of Hacks." Wired. August 18, 2017. Accessed January 10, 2018. <https://www.wired.com/story/hbo-hacks-game-of-thrones/>.
- ^{xv}Newman, Lily Hay. "The Worst Hacks of 2017." Wired. January 05, 2018. Accessed January 10, 2018. <https://www.wired.com/story/worst-hacks-2017/>.
- ^{xvi}McGann, Hilary and Ralph Ellis. "Heathrow Airport launches probe after USB stick with security files found." CNN. October 29, 2017. Accessed January 10, 2018. <http://www.cnn.com/2017/10/29/europe/heathrow-airport-security-usb-stick/index.html>.
- ^{xvii}Menn, Joseph and Dustin Volz.
- ^{xviii}Perloth, Nicole and Matthew Haag.
- ^{xix}Burgess, Matt and James Temperton.
- ^{xx}Peterson, Andrea.
- ^{xxi}Muncaster, Phil. "Google Hit by Insider Data Breach." Infosecurity Magazine. May 10, 2016. Accessed January 10, 2018. <https://www.infosecurity-magazine.com/news/google-hit-by-insider-data-breach/>.
- ^{xxii}McGann, Hilary and Ralph Ellis.
- ^{xxiii}"BlackBerry Workspaces Isn't Just Secure – It Enables Your Business to Be More Productive." BlackBerry. September 12, 2017. Accessed January 10, 2018. <https://us.blackberry.com/enterprise/forms/gartner-critical-capabilities-for-content-collaboration>.
- ^{xxiv}"Forrester Wave EFSS Hybrid Solutions." BlackBerry. April 26, 2016. Accessed January 10, 2018. <https://us.blackberry.com/enterprise/forms/Workspaces-Forrester-EFSS-Wave>.

