The Buck Stops Where?

ASSESSING THE CYBERSECURITY PERFORMANCE OF THE FINANCE SUPPLY CHAIN

BITSIGHT®
The Standard in SECURITY RATINGS

INTRODUCTION

An increasing number of data breaches originate with the compromise of a key vendor or business partner. This trend was heightened with the spread of NotPetya ransomware which first emerged when the software update process of an accounting software provider in Ukraine was hijacked[1]. With digital services being increasingly outsourced, reducing cyber risk posed from a growing number of vendors and suppliers is more important than ever.

For years, the Finance industry has been a trailblazer in managing the risk posed by vendors, suppliers, and business partners. As we have also detailed in previous BitSight Insights reports[2] over the last four years, this industry has maintained a strong security posture in comparison to others. Given that the Finance industry is a leader in managing third-party cyber risk, how secure is their supply chain, and where do weak links lie? Are the companies in their supply chain meeting the same security standards they hold for their own organization? These questions are relevant not only for Finance organizations, but for all organizations that need to reduce third-party cyber risk.

To answer these questions, BitSight researchers looked at the security performance of more than 5,200 Legal, Technology, and Business Services global organizations whose security ratings are tracked and monitored by hundreds of Finance firms using the BitSight Security Rating platform. The organizations across these industries represent a set of critical vendors and business partners in Finance's supply chain, consisting of: legal organizations, accounting and human resources firms, management consulting and outsourcing firms, and information technology and software providers.

It is important to note that according to BitSight's responsible disclosure policy[3], we do not publish the security performance for any one company: all performance is aggregated and anonymized. Understanding some of the common risks that exist in supply chains can help organizations across all industries manage third-party cyber risk. Security and risk professionals can use these findings to help shape the way they conduct vendor risk assessments in order to identify immediate risk that may impact their organization.

KEY FINDINGS

1. A significant security performance gap exists between these Finance firms and companies in their supply chain: the mean rating for Finance companies was at least 30 points higher than the mean of companies in their supply chain.
2. Companies in the Finance supply chain with a combined Desktop Software Grade of "B" or lower were more than twice as likely to have had a machine compromise in the past year.
3. One in five Business Services organizations in the Finance supply chain has at least one instance of Windows XP on their network: the presence of outdated desktop operating systems and browsers increases the likelihood of a publicly disclosed breach.
4. Nearly 1 in 4 Technology and Business Services firms in the Finance supply chain is running unsupported Windows IIS on servers, known to be vulnerable to exploits.
5. Peer-to-peer file sharing occurs in over 20% of Technology and Business Services firms in the Finance supply chain, but less than 10% of Legal organizations.

OVERALL SECURITY POSTURE

A significant gap exists between Finance firms and companies in their supply chain. This is noteworthy as organizations should strive to hold their vendors to the same security standards set for their own organizations. As of September 1st 2017, the mean rating of Finance companies in this study was 710. However, the mean ratings for Legal Organizations, Technology Firms, and Business Services firms were 680, 670, and 660 respectively. While managing third-party cyber risk is a relatively new initiative for businesses, this performance gap illustrates the challenge Finance firms have in raising the security performance of key vendors and business partners.

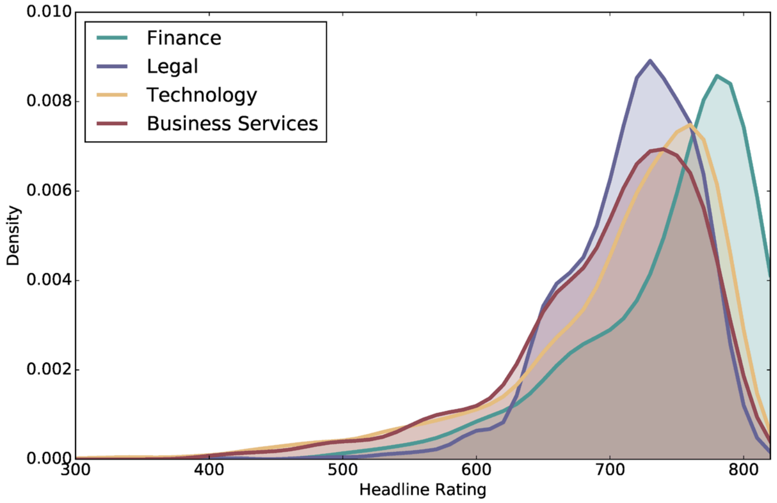


FIGURE 1

The spread of BitSight Security Ratings amongst Finance Firms and monitored Legal, Technology, and Business Services organizations as of September 1st 2017.

We recently reported that the Legal sector has emerged as a top-performing industry in security performance. Legal firms in the Finance supply chain have maintained a high level of performance, and are much closer to meeting the performance level of peer Finance organizations.

Technology firms have demonstrated improvement over time, yet a large gap exists between these companies and Legal organizations. Out of these three main industries, Business Services companies present the highest level of risk for the Finance industry. Performance in this industry is particularly problematic given that these firms likely have access to sensitive data on the employees of firms they work with.

INDUSTRY COMPOSITION

Technology

Computer & Network Security | Software | Information Technology & Services

Business Services

Accounting | Human Resources | Staffing & Recruiting | Management Consulting | Outsourcing

Legal

Law Practices | Law Firms | Legal Services

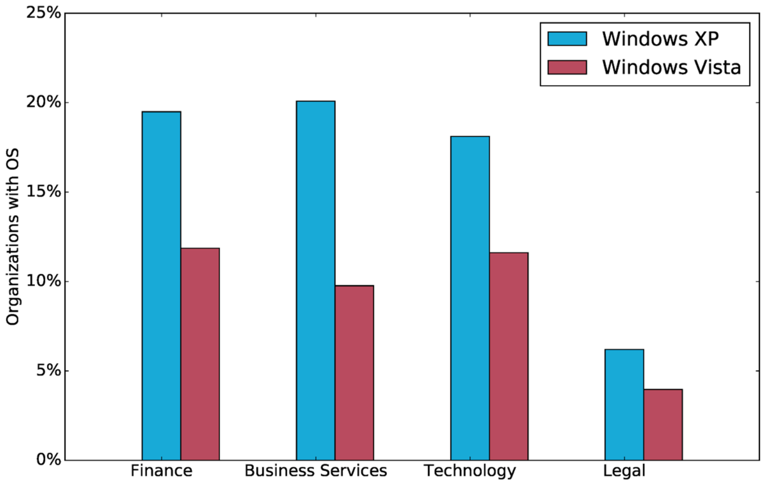
WHO’S STILL RUNNING XP & VISTA?

The previous BitSight Insights report, A Growing Risk Ignored: Critical Updates[4], explored the risks of outdated systems on corporate networks. BitSight assessed more than 35,000 companies and found that companies with more than 50% of their Desktop Operating System or Internet browsers out of date were *2-3 times more likely to experience a publicly disclosed data breach.*

In this study, we looked at Finance organizations and members of their supply chain who are running at least one instance of Windows XP or Windows Vista on their networks. Both of these operating systems are no longer supported[5] by Microsoft and generally do not have security patches available to protect against new risks[6].

FIGURE 2

The percentage of companies running at least one instance of Windows XP or Windows Vista as of July 1st, 2017.



With the exception of Legal organizations, Finance’s supply chain has similar rates of outdated operating systems on their networks. As of June 2017, nearly 20% of Finance, Business Services, and Technology firms had at least one instance of Windows XP on their corporate network. Roughly 10% of these companies are also running Windows Vista. Legal organizations are an outlier in this area, performing better with far less than 10% of firms running XP or Vista on their networks.

THE CORRELATION BETWEEN OUTDATED SYSTEMS AND MACHINE COMPROMISE

What does it mean for Finance companies who work with firms that run unsupported Operating Systems and Browsers? Those in the Finance supply chain with a Desktop Software Grade of “B” or lower were *more than twice as likely to have had a machine compromise in the past year*. This means that outdated desktop operating systems and browsers that exist within a supply chain are correlated to more immediate risks of machine compromise and data loss.

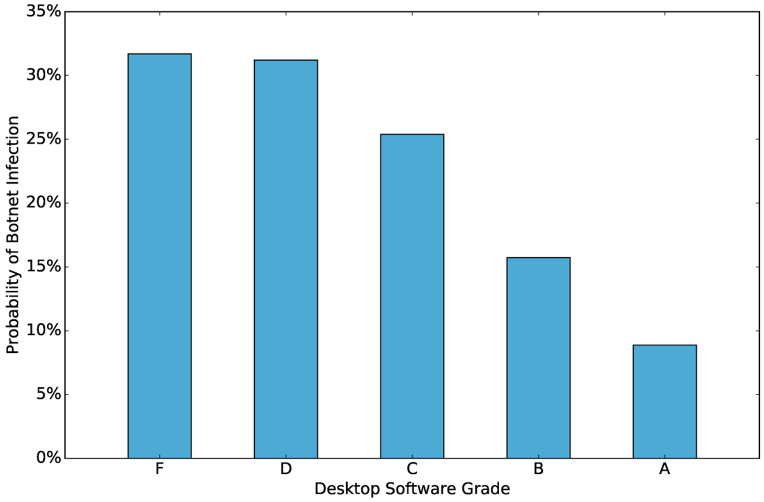


FIGURE 3

The BitSight Desktop Software Grade for Business Services, Technology, and Legal firms as of July 1st, 2017. Desktop Software grades are comprised from the number and severity of outdated browsers and operating systems a company has on their network.

The prevalence of outdated systems found on networks for companies in the Finance supply chain should prompt a discussion about why companies are running outdated software and their timeline for updates. Beyond this discussion, organizations should continuously monitor their vendors to ensure progress is being made in this area, and that the number of outdated systems connected to a network declines.

OUTDATED SERVER SOFTWARE

If an organization is sharing data with its vendor, the data is likely being stored on an on-premise server, or through cloud providers. It is important for Finance firms to know if a vendor's servers are running unsupported or out-of-date software, which may increase the likelihood of data compromise. A prime example is the "Panama Papers" breach of law firm Mossack Fonseca: the law firm was reportedly running outdated versions of popular open source web server software Drupal and WordPress at the time of breach[7].

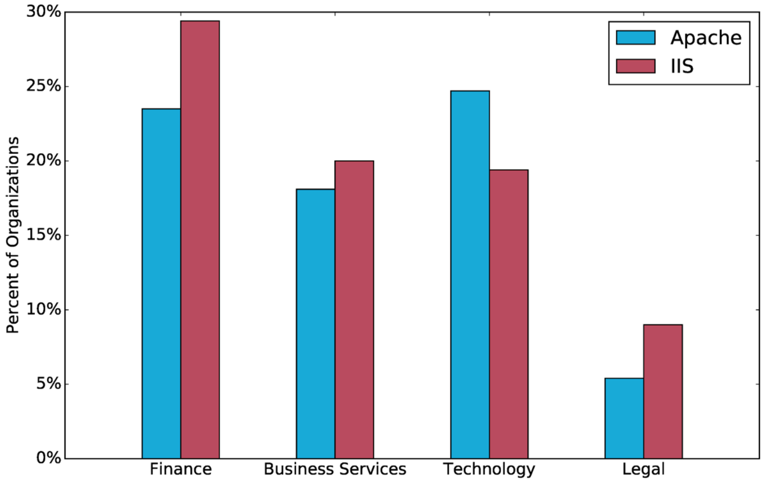


FIGURE 4

The percentage of companies running at least one unsupported instance of Apache or Windows IIS on a server as of July 1st, 2017.

One of many NSA exploits leaked by the Shadow Brokers takes advantage of unsupported server software to allow attackers to remotely execute code. Dubbed “ExplodingCan”, the exploit uses a known flaw in Windows IIS 6.0 servers that have[8] an extension enabled for remote content creation and management. This vulnerability can allow attackers to implant ransomware and other malware remotely on servers susceptible to the exploit.

Server Software is one area where Finance is actually falling short compared to their supply chain. Nearly 30% of Finance firms have one instance of outdated Windows IIS on their networks, compared to less than 10% of companies in the Legal sector. This rate is also lower for Business Services and Technology Firms, with nearly 20% of companies in both of these industries having at least one server with outdated Windows IIS. These industry rates are also comparable for unsupported versions of Apache, which has had 15 documented CVEs reported since 2015[9]. Ensuring that servers are properly configured and up-to-date is an area where all organizations have room for improvement.

PEER-TO-PEER FILE SHARING

Previous BitSight research shows that high levels of file sharing activity correlates to a higher rate of system compromise[10]. Finance organizations set an impressive standard with less than 1% exhibiting torrent downloads on corporate networks. Legal organizations also have very little torrenting activity: under 10% of firms in this industry have torrents, and just 3% have downloaded an application.

The rate is over twice as high for Business Services and Technology firms: 22% of Business Services firms and 23% of Technology firms have torrented. Furthermore, 10% or more of companies in these industries have downloaded an applications (such as Microsoft Office and Adobe Suite applications) which can increase the likelihood of a potentially-unwanted application being introduced onto a network. Overall, peer-to-peer file sharing activity may be indicative of other lax security policies for an organization.

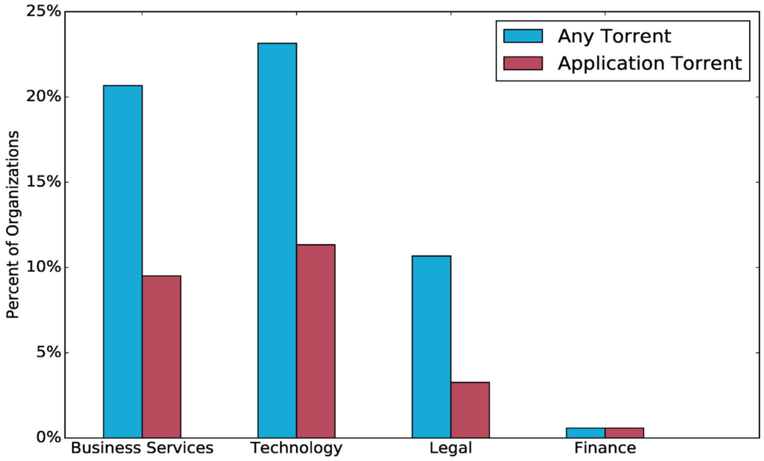


FIGURE 5

The percentage of companies who had torrent activity using the BitTorrent protocol corporate networks between July 1st 2016 to July 1st, 2017.

BUSINESS RECOMMEDNATIONS

1. Understand Endpoint Security of Critical Vendors

Ensure that devices are up-to-date with supported operating systems and browsers. Given that companies with outdated systems are more likely to exhibit system compromise, the risk of data loss and exfiltration is heightened if operating systems and browsers are outdated. Specifically, organizations should start by identifying vendors who have Windows XP and Vista running on their networks and ask for a timetable on when systems will be updated.

2. Scrutinize Server Security

Confirm with vendors that software running on their servers is also up-to-date. Organizations should especially inquire into the software running on any servers that contain their data: it is the most immediate path to data compromise.

3. Look out for Peer-to-Peer File Sharing

Peer-to-Peer file sharing can introduce malicious applications onto networks and lead to system compromise. Organizations should look to work with vendors who hold the same policies on file sharing as their organization. If a vendor exhibits peer-to-peer file sharing on their network, ask to review their file sharing policies.

4. Set a High Bar For Your Vendors, Suppliers, and Business Associates

Many organizations set a standard of security performance for their third parties by strengthening contractual language. Organizations can go even further by demonstrating a strong security posture over time and collaborating with third parties to improve their level of performance.

CONCLUSION

Third party risk management is imperative today for organizations large and small. Senior executives and Boards of Directors are increasingly asking for updates into their vendor risk management programs and looking for demonstrable progress in reducing third party cyber risk. By 2020, Gartner estimates that 75% of Fortune 500 companies will treat vendor risk management[11] as a board-level initiative to mitigate brand and reputation risk. Moreover, cyber insurers are beginning to inquire not only about the security posture of applicants, but their third and fourth parties as well. For many organizations, it will be imperative to demonstrate reduced cyber risk stemming from vendors, suppliers, and business partners to internal and external stakeholders.

While Finance organizations tend to have more sophisticated vendor risk management programs, there is much work to be done to close the performance gap between their own organizations and their immediate business ecosystem. The findings of this report are not only relevant for the Finance sector; companies across all industries who share data and network access should place a great deal of scrutiny on the security culture of the third and fourth parties in their business ecosystem. Ensuring that your vendor's systems are up-to-date and that their employees are not engaging in risky peer-to-peer file sharing is one way to reduce immediate third party cyber risk.

METHODOLOGY

This study looked at 5,281 companies monitored by hundreds of Finance organizations using the BitSight Security Rating platform. Data on the overall security posture of Finance firms and companies they monitor was processed as of September 1st, 2017. The percentage of companies running Windows XP or Windows Vista was processed as of July 1st, 2017. Data on the combined BitSight Desktop Software Grade was processed as of July 1st, 2017. Data on the percentage of companies running Apache or Windows IIS on servers was processed as of July 1st, 2017. The percentage of companies who had torrent activity on corporate networks was taken between July 1st 2016 to July 1st, 2017.

REFERENCES

1. “Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide” https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/

2. BitSight Research & Insights https://www.bitsighttech.com/research-insights

3. BitSight Responsible Disclosure Policy https://www.bitsighttech.com/responsible-disclosure

4. “A Growing Risk Ignored: Critical Updates” https://info.bitsighttech.com/bitsight-insights-a-growing-risk-ignored-critical-updates

5. “Windows XP support has ended” https://support.microsoft.com/en-us/help/14223/windows-xp-end-of-support

6. “Windows Vista support has ended” https://support.microsoft.com/en-us/help/22882/windows-vista-end-of-support

7. “Cybersecurity Lessons Learned From ‘Panama Papers’ Breach” https://www.forbes.com/sites/jasonbloomberg/2016/04/21/cybersecurity-lessons-learned-from-panama-papers-breach/#401300202003

8. “ExplodingCan NSA exploit menaces thousands of servers” https://www.itnews.com.au/news/explodingcan-nsa-exploit-menaces-thousands-of-servers-463985

9. CVE Details for Apache https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/Apache-Http-Server.html

10. “Peer-to-Peer Peril: How Peer-to-Peer Sharing Impacts Vendor Risk & Security Benchmarking” https://info.bitsighttech.com/how-peer-to-peer-file-sharing-impacts-vendor-risk-security-benchmarking

11. Magic Quadrant for IT Vendor Risk Management https://www.gartner.com/doc/3748994/magic-quadrant-it-vendor-risk