VENDOR VULNERABILITY:
HOW TO PREVENT THE SECURITY RISK OF THIRD-PARTY SUPPLIERS
Between November and December 2013, the U.S. retailer Target was the subject of one of the largest data breaches in history. Hackers introduced malware to the card reading systems in nearly 1,800 Target stores during the busiest retail season of the year. They captured the credit and debit card information of approximately 40 million customers. How did the hackers manage to compromise such a large system and get away with so much valuable data? The answer lies with Fazio Mechanical Services (FSM), a heating, ventilation and air conditioning (HVAC) contractor in Pittsburgh. FSM provided electronic billing services, contract submissions and project management services to some Target stores and had access to its network. The hackers stole FSM’s credentials and used them to gain access to Target’s systems.

The Target breach powerfully illustrates how businesses in any industry are potentially at risk from the third parties with which they work. Without a robust solution for managing, controlling, or monitoring a vendor’s access to its network, Target effectively left the back door open for hackers to walk in.

But since 2013, how much has really been done to tackle the issue of vendor access management? Is it something for which businesses are actively considering and deploying solutions? Or has it slipped from people’s minds, leaving businesses and their sensitive data at extreme risk?

To find out, we surveyed hundreds of IT and Security decision makers who have oversight of third-party access to their organization’s network. We found that, while vendor access management is something that most are aware of, few have pursued the solutions that would guarantee the safety of their sensitive business data from possible third-party breaches. And, with the number of third-party vendors a business engages set to rise dramatically over the next few years, time is running out to safeguard against this very real threat.

69% of respondents say they definitely or possibly suffered a security breach resulting from vendor access within the last year.
RESEARCH METHODOLOGY

608 key decision makers with visibility over the processes associated with enabling any external parties to connect to their systems remotely completed a survey during February 2016. Those surveyed were all IT professionals across Operations, IT Support/Helpdesk, IT Security or Network/General IT roles. Respondents were from a multitude of industries, including Professional Services, Finance, Manufacturing, Healthcare, Retail and the Public Sector. The survey was conducted across the United Kingdom, the United States, Germany and France.
The discussion around vendor vulnerability is extremely relevant when one considers the vast network of third-party suppliers most organizations possess. Respondents to our survey reported that, on average, 89 vendors are accessing their company’s network every single week. Respondents reported that 45% of third-party vendors who have access to their internal networks logged in within the past year.
Vendors and third-party suppliers are clearly vital to organizations. They are part of the ecosystem in which modern businesses must operate, and this ecosystem will only grow in scale and importance. Nearly three quarters (71%) of respondents are expecting their companies to become more reliant on third parties in the next two years.

But as the complex network of suppliers and third-party vendors within your organization grows, so too does the risk. Without proper policies for the control and management of vendor access to your network, there is a security threat to not just your business, but to your employees and customers.

ON AVERAGE, 89 VENDORS ARE ACCESSING A COMPANY’S NETWORK EVERY SINGLE WEEK.
It’s not that organizations don’t understand these risks. Amongst those surveyed, there was a general awareness of the threats posed by ineffective management and poor visibility of vendor access. But it was clear from our respondents that not enough is being done to address the risks and concerns around vendor vulnerability.
SO WHAT MAKES A COMPANY VENDOR VULNERABLE?

- **Non-stratified access to the network**

  Just under half (44%) of those surveyed reported an ON/OFF approach to vendor access, rather than employing varying levels of access for different vendors. This equates to roughly every other company simply welcoming vendors into their entire network or shutting them out completely.

  This is a wildly risky approach. Most vendors do not need access to the entirety of your network and vendors should only be given access to specific systems or applications based upon the services they provide to your organization. This should be supplemented with bespoke logins, company credential policies and secure remote access tools.

- **High levels of (unwarranted) trust in third-party vendors**

  Many are placing too much trust in the vendors they work with. An astonishing 92% of respondents say they trust vendors completely or most of the time. But there is a growing realization that, when granting a vendor access to your network, this decision needs to be based on more than just blind faith. More than two-thirds (67%) of respondents believe that they tend to trust vendors too much.

  Organizations need robust controls and checks to mitigate the security risk of vendors. Do you know what technology and tools third-parties are using to access your networks? Can you see when they’re accessing your systems and what they’re doing? Are your vendors sharing simple passwords among employees or employing security best practices, such as multifactor authentication and credential rotation?

  In the current climate, it is no longer enough to simply trust that a vendor has the security policies in place to defend against threats.

- **Lack of visibility of vendor access to network**

  With so many vendors accessing an organization’s network on a weekly and annual basis, it is absolutely imperative to have visibility of which vendors are logging in and when. But when pressed on this matter, only 35% of respondents are very confident in knowing the actual number of vendors accessing their systems, and just 34% know the number of individual log-ins that can be attributed to vendors.

  Perhaps most shockingly, 69% say they definitely or possibly suffered a security breach resulting from vendor access within the last year. The fact that many organizations cannot even determine for certain if a breach was the result of vendor access is a sobering thought, and proof that visibility is a key issue when it comes to vendor vulnerability.

  These numbers reveal a huge gap in many organizations’ ability to limit their exposure to security breaches. Without the ability to establish an audit trail of exactly which vendors have been accessing your network, you cannot be sure if one of their accounts has been compromised. In the event a breach does occur, your business will have to shoulder all responsibility for the security failure.
**Out of Date Policy and Enforcement Around Third-Party Access**

Two thirds of respondents reported that they find it difficult to keep on top of the changing security threats to their company. This is reflected in the fact that more than half (55%) of those surveyed have not reviewed their policy around third-party access in the last two years. Just 51% said they enforce policies around third-party access.

It can feel like a fool’s errand to keep your vendor access policy up-to-date with every emerging security risk. These things change daily, sometimes hourly. But the reality is that an up-to-date policy on third-party access is essential to protect your business. More importantly, every policy put into place should have a corresponding enforcement strategy and tools that make enforcing evolving policies simple and effective.

**74% Believe that Third-Party Vendor Selection Overlooks Key Risks, with 64% Saying that Their Organization Focuses More on Cost Than Security When Outsourcing.**

More than half (56%) of respondents think that threats around vendor access are not taken seriously enough in their organization. Indeed, nearly three quarters (74%) believe that third-party vendor selection overlooks key risks, with 64% saying that their organization focuses more on cost than security when outsourcing.

This is a difficult issue to negotiate, as it is as much about effecting cultural change within the business, as it is about providing a solution for vendor access management. But if cost is such a concern for the powers that be, then perhaps it bears mentioning that the Target breach reportedly cost the company $252 million. The cost of not taking the threat seriously will be far greater than the cost of preventing third-party security risks in the first place.
It is clear from the research that vendor vulnerability is a significant risk to any organization that engages with a third-party supplier and allows them access to their network. But time is running out for businesses to find a solution. Greater risks are on the horizon.
Respondents in our survey are nervous about future security breaches. More than three quarters (77%) believe their company will experience a serious information breach within the next two years as a result of vendor activity on their networks. Worryingly, 64% of those surveyed fear that this will happen within the next year.

**77% BELIEVE THEIR COMPANY WILL EXPERIENCE A SERIOUS INFORMATION BREACH WITHIN THE NEXT TWO YEARS AS A RESULT OF VENDOR ACTIVITY ON THEIR NETWORKS.**

As an organization’s network of vendors and third-party suppliers grows, so does the risk of a potential breach. Vendors will increasingly engage third-party suppliers of their own to carry out work on your organization’s behalf. However, 72% of respondents see this “fourth party risk” as a major concern for the future. It is hard enough to manage network access for the vendors you know about, let alone the ones that you don’t. The growing complexity of vendor networks presents significant challenges in this regard.

Another key concern is that the devices that connect to your networks will exponentially increase in the coming years. Nearly three quarters (74%) of those surveyed are worried about breaches originating from connected devices over the next year. This does not just include smartphones and other mobile devices. With the Internet of Things and the proliferation of internet-enabled peripherals, the number of entry points through which an attack could occur will grow significantly.

IT managers, CIOs and CSOs know what is needed to reduce the risk. More than half (55%) think their business will be better protected if they have a policy where vendor access is stratified according to perceived levels of risk. Nearly eight in ten people (78%) believe third-party vendor breaches can only be effectively reduced through access control measures at a people, process, and technology level. And there is a general consensus that higher quality controls throughout the vendor lifecycle (57%), efficiency in the management and monitoring of vendors (52%) and effective monitoring of third-party vendor risks (52%) will be key considerations in safeguarding against vendor data breaches.

All that remains is to translate awareness into action.

---

**FIG 6. TIMEFRAME UNTIL A SERIOUS INFORMATION BREACH OCCURS**

<table>
<thead>
<tr>
<th>Timeframe</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Already happened</td>
<td>11%</td>
</tr>
<tr>
<td>Less than 6 months</td>
<td>29%</td>
</tr>
<tr>
<td>6 months - 1 year</td>
<td>24%</td>
</tr>
<tr>
<td>1 - 2 years</td>
<td>14%</td>
</tr>
<tr>
<td>Longer than 2 years</td>
<td>6%</td>
</tr>
</tbody>
</table>

**FIG 7. KEY CONSIDERATIONS IN PROTECTING AGAINST SECURITY BREACHES**

- Higher quality / tighter controls throughout third-party vendor lifecycle: 57%
- Speed / efficiency in the management & monitoring of vendors: 54%
- Effective monitoring of third party vendor risks: 52%
- Consistency in how third party vendor access is managed: 42%
- Reduced cost & time of managing third party vendor risk: 37%
- Improved regulatory compliance: 19%
The good news is that all hope is not lost for organizations, as there are solutions available that will help them manage vendor access to their networks. Many of these solutions enable security professionals to control, monitor, and manage privileged access to critical systems by authorized employers, contractors, and third-party vendors.

There is little time to waste, however, and when investigating a Privileged Access Management solution, you should ensure that it has the following capabilities:

1. The ability to account for all vendors with access to systems, the data or applications to which they have access, and why they need it. This information should be regularly reviewed to determine whether vendors still require that level of access.

2. The ability to stratify access to individual vendors (even individuals within the vendor’s organization) so they can log into only the applications or systems necessary for their role.

3. The ability to identify when a vendor’s access may have been compromised and revoke or reduce network access to specific vendors immediately.

4. The ability to enforce processes around who within your organization can grant third-party vendor access to your systems.

5. The ability to control and monitor additional vendors who may be accessing your systems, such as fourth-party subcontractors.
Bomgar is the leader in Secure Access solutions that allow organizations to connect fearlessly to people and technology around the world. Bomgar provides leading remote support and privileged access management solutions that strengthen security while increasing productivity. Bomgar solutions help support and security professionals improve business performance by enabling secure, controlled access to nearly any device or system, anywhere in the world. More than 10,000 organizations across 80 countries use Bomgar to deliver superior support services and manage access to valuable data and systems.

To find out how Bomgar’s Secure Access solutions can help your business operate more securely, please visit www.bomgar.com