In December 2016, Yahoo revealed that more than 1 billion user accounts had been compromised during a breach in August 2013, the largest ever in history. This was only a few months after the company confirmed that the personal data of 500 million accounts had been stolen in 2014. And in May 2016, over four years after LinkedIn was notoriously hacked, 117 million email and password combinations appeared for sale on the dark web.

These costly and brand-impacting security breaches serve as a stark reminder that sensitive systems and data within organizations are under constant threat. For most, suffering a serious information security breach is no longer a question of if, but when.

Despite being aware of the threats, most organizations still allow a myriad of internal and external parties to access their most valuable systems and data. Many are placing a lot of trust in both employees inside their business and third parties outside of it without a robust means of managing, controlling, and monitoring the privileged access that these individuals, teams, and organizations have to their network. Even those that have some solutions and policies in place to mitigate the risk need to continually reassess if those solutions can defend against evolving threats.

This became evident when we spoke to hundreds of IT and Security professionals with oversight of who connects to their organization’s network. More than half (52%) expect their organization to be breached within the next year. For 15%, a breach has already occurred.
Our respondents outlined two primary, yet distinct, threats:

1. **Insiders**
   Employees or people acting as an employee for the business, including freelancers or on-premises contractors. More than two thirds (67%) say that a breach originating from an insider (whether malicious or unintentional) is their greatest security threat.

2. **Third parties**
   External vendors or suppliers granted access to business systems, including outsourcers. Three quarters (75%) of security and IT professionals say breaches like those at Yahoo and LinkedIn have made them more aware of the need to better control third-party access to their systems.

This report will outline the ways in which both insiders and third parties present security risks to organizations, as well as the approaches and solutions security professionals can adopt to protect their valuable data.
key decision makers with visibility over the processes associated with enabling external parties to remotely connect to their systems completed a survey in February 2017. Those surveyed were all IT professionals across Operations, IT Support/Helpdesk, IT Security or Network/General IT roles. Respondents were from a range of industries, including Manufacturing, Finance, Professional Services, Retail, Healthcare, Telecoms and the Public Sector. The survey was conducted across the United Kingdom, the United States, Germany and France.
The threat from within: the paradox of trust and risk. It’s a fundamental aspect of information security that certain employees and contractors must — by virtue of their function or role — be granted privileged access to, and rights within, corporate systems. This is a relationship built on trust, and most of the time employees with privileged access are deemed trustworthy.
Our respondents trust the insiders with elevated access to their systems most of the time, but few trust all of them all of the time. Despite placing a lot of trust in employees with privileged access, security professionals are paradoxically aware of the numerous risks that these individuals pose to the business. While the threat of employees exploiting company data, either for personal gain or deliberate sabotage, were acknowledged by IT decision makers, they were not primarily worried about breaches of malicious intent. The top concerns were that a breach could be caused by employees unintentionally mishandling data (for example, sending sensitive information via email to the wrong person), or that an employee’s administrative access or privileged credentials could be easily phished by cyber criminals.

It only takes one employee to leave a business vulnerable. It’s crucial that organizations control, manage, and monitor privileged access to their systems to mitigate that risk.

Yet businesses are falling behind. Only 37% are very confident they have complete visibility of which employees even have privileged access, which might explain why a third (33%) of security professionals believe that some of their ex-employees could still have access to the corporate network. Similarly, a mere 35% can identify specific threats from employees with elevated privileges, and just 34% are very confident that they have reporting on the individual user activity of each privileged employee.

These facts tell us that many organizations can’t adequately manage the risk related to privileged accounts. The best way to deal with the risk is to use a complete Privileged Access Management solution to manage and control how users connect to privileged systems, define and manage what they can access and do once connected, and record and monitor sessions for unexpected activity. Insider data breaches — whether malicious or unintentional — can go on for months or years without being detected, increasing the potential damage to the company.

90% of security professionals trust employees with privileged access most of the time but only 41% trust these insiders completely.
SECURITY SOLUTIONS ARE INHIBITING PRODUCTIVITY

We’re not suggesting that IT decision makers are doing nothing to defend their businesses from insider threats. No doubt many of the people reading this will have invested significant sums of money in technology for that exact purpose. However, when security solutions slow down or restrict employees, they will find work-arounds to avoid or bypass locked-down IT processes. Security managers have noticed a variety of security-compromising bad habits that employees regularly display [FIG2].

This suggests that employees aren’t malicious in their bad behavior. Rather, they simply cut corners to speed up their own productivity.

Generally, employees want to be productive and responsible at work. But these two are not always complementary goals. When workers are faced with security measures that seemingly hinder their efficiency, they’ll use shortcuts without considering the risks. What’s gained in a few minutes of extra productivity then opens the door to threats. And while some privileged access management solutions address such bad behavior, many don’t go far enough.

What’s needed are solutions that prioritize both productivity and usability. A solution that can be seamlessly integrated into the applications and processes that employees already use will not only promote good security behavior, but ultimately keep organizations safe.

69% Staying logged on
57% Sending files to personal email accounts
55% Writing down passwords
55% Downloading data onto an external memory stick or drive
53% Logging on over unsecured WiFi (e.g. from Starbucks)
46% Telling colleagues their passwords

[FIG2] PROLIFERATION OF SECURITY ISSUES
DEALING WITH PRIVILEGE SPRAWL

The way in which we think about privileged access is changing. Traditionally, privileged access has been viewed as employees, applications, and systems with “IT admin” credentials. But that definition is evolving. The amount and variety of access that individuals have is expanding and what is considered “privileged” or sensitive for a company is no longer just payment or customer data.

Consider the reputational damage that can be done if someone gained control of a retailer’s Twitter handle by phishing credentials from someone in the marketing department. Or if an attacker gains access to a manufacturing floor system at an auto maker. Or if an attacker got into a lawyer’s confidential client emails using an assistant’s credentials.

Businesses need to consider how they will manage this privilege sprawl. It is a challenge that affects not just insiders, but third parties too. External suppliers and vendors are also seeing the breadth and depth of their access to a business’ systems grow.

Service desks and managed service providers, for example, could be considered a vulnerability for many businesses. They are usually high turnover organizations with a less mature approach to security, but they have extraordinary access to business systems. With these kind of outsourcing arrangements becoming larger and more common, the way that privilege is managed for them needs to evolve.
Data breaches as a result of third party access are widespread. External suppliers continue to be an integral part of how most organizations do business. On average, 181 vendors are accessing a company’s network every single week, more than double the number from 2016. In fact, 81% of companies have seen an increase in third-party vendors in the past two years, compared to 75% in the previous year.
With so many third parties granted access to an organization's systems, it is perhaps no surprise that more than two thirds (67%) have experienced a data breach as a result of vendor access. While this is a small drop from last year's findings (69%), it is still common enough to be a major cause for concern.

While this has prompted 66% of security professionals to say that they trust third-party vendors too much, action has not followed this recognition. Processes to control and manage privileged access for vendors remain lax, as evidenced by the fact that only 34% of respondents are totally confident that they can track vendor log-ins, and not many more (37%) are confident they can track the number of vendors accessing business systems.

It's shocking to learn, then, that more than half (55%) of organizations rely on a single employee to manage third-party access rights. If so few businesses have a handle on how many third parties have access to their network and what those vendors are doing with that access, then having one person managing it all is not a sustainable solution and represents serious risk.

As the vendor ecosystem grows, such an important function will need to be better managed through robust solutions and processes that provide visibility and control to a larger group of people. Managing the privileged access and credentials for such a wide network of third parties also needs to be seamless and easy to administer to keep both employees and vendors productive while reducing risk.

**Vendors Accessing a Company’s Network Every Week**

<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>89</td>
</tr>
<tr>
<td>2017</td>
<td>181</td>
</tr>
</tbody>
</table>
MORE COMPLEX THREATS ARE STILL BEING MET INADEQUATELY

As with insiders, third-party privileged access presents a multitude of risks to network security (see Fig 4). Many of the threats are similar, from third parties sharing passwords amongst their teams, to a lack of a visible audit trail for activity on the network. Some are unique to third parties, such as ‘fourth party’ risk, in which vendors themselves hire subcontractors and give them access to a company’s network.

It is encouraging to see that many security professionals are tailoring vendor access by admitting them only to specific systems or applications. Two thirds (66%) of businesses are now doing this, a 10% increase from 2016. However, this still leaves more than a third (34%) of organizations that are providing just ON/OFF access – either full access or no access. Giving external parties full access — such as via a VPN — to a network where they can access systems they have no need to use is a potentially disastrous approach.

FIG 4. WHICH OF THESE DO YOU CONSIDER THE MOST SIGNIFICANT RISKS TO NETWORK SECURITY?

- Third party vendors sharing log-in and passwords amongst team to access your network: 32%
- Lack of incident response processes to report and manage third party vendor data breaches: 30%
- Third parties outsourcing elements of work to subcontractors, increasing the level of exposure: 28%
- Third party vendors do not recognize the importance of data security, with a lack of systems and procedures to manage data securely: 27%
- Lack of visibility / audit trail of third party vendor activity on your network: 26%
As with insiders, a ‘least privilege’ policy, in which a user can access only the information or resources necessary to their function, is the best practice. Access rights need to be more than a simple yes or no. Similarly, to combat the growing ‘fourth party’ risk, security professionals should ensure they are able to track and monitor individual users even if they’re leveraging secured, shared credentials.

**PEOPLE AND PROCESS**

Technology is just one component of security, and people and processes also have a significant role to play. While businesses are generally good at adopting new technology, they often struggle with deploying and evolving security processes and training.

The vast majority (53%) last reviewed their policy two years or more ago. Less than half (47%) of companies have reviewed their access policy in the last two years. Given the speed that the risk landscape evolves, this is an alarmingly insufficient approach.

Similarly, businesses need to do more to make employees aware of their security policies and best practices. Only around half (54%) of organizations conduct annual training to keep insiders aware of security processes and, shockingly, only 53% include this training as part of induction for new employees. One must ask the question: if an employee hasn’t been trained to know what a threat looks like, how will they be able to protect themselves?
Security professionals must balance the business needs of those accessing their systems — whether insiders or third parties — with security. It’s no longer enough to just train your users and trust they’ll follow the rules, or to lock down parts of a network even if it impacts productivity.
FIVE WAYS TO DEAL WITH THE SECURITY RISKS OF INSIDERS AND THIRD PARTIES

To truly defend businesses from threats both within and from the outside, a variety of approaches can be adopted:

1. **ENFORCE ‘LEAST PRIVILEGE’ AS THE STANDARD**
   Instead of giving users all-or-nothing access, privilege must be granted based on specific user needs and scenarios. A solution needs to allow for different levels of individual access, with a broad scope for what that means. You should be able to control access based on, for example, function, team, vendor, location, time of day, and more.

2. **CONSIDER THE USER EXPERIENCE**
   Security solutions need to be usable. Access to systems should be granted in seconds, while still providing all of the checks and balances to mitigate threats. Security teams can’t slow things down in the name of security as this risks productivity and insiders will find riskier work-arounds. Give people something that’s easy to use, and that fits (or even improves) how they do their day-to-day jobs. This approach requires security and IT professionals to involve end-users in the early stages of designing new policies or selecting new technology.

3. **IMPLEMENT SEAMLESS WORKFLOW PROCESSES**
   Companies don’t have large teams to manage access rights for the growing number of privileged insiders and vendors. Solutions to grant and revoke privileged credentials and permissions need to be easy to administer and use, and integrate seamlessly with existing environments.

4. **MONITOR, RECORD AND ANALYZE BEHAVIOR**
   As the environment becomes more complex, technology can help you comply with regulations requiring that all activity and behavior is monitored. You should be able to identify every individual that accesses sensitive systems and what they are doing, as well as sound the alarm if they are doing anything malicious. All of this information needs to be recorded so there is a clear audit trail.

5. **REVIEW POLICIES AND TRAIN PEOPLE REGULARLY**
   Technology can help make security easier, but it is just one aspect of the entire solution. People and processes must support this too. Review your security policies often, and make sure new and existing employees are trained on them. Each employee or contractor needs to understand how their day-to-day actions can help protect the business from threats.
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 more, contact Bomgar at www.bomgar.com