Rethinking Insider Risk in the Gig Economy
INTRODUCTION

More and more companies are relying on gig, contract and freelance workers to scale their business. Fully 1 in 5 people now belong to the contract workforce, according to a 2018 NPR/Marist poll.¹

The global pandemic has only accelerated this trend. In Q2 2020 alone, freelance job postings in the U.S. rose 41% compared to the same period in 2019.² Gig workers already make up 43% of the total U.S. workforce according to recent estimates.³

By 2027, gig workers may account for half of the total U.S. workforce.⁶

It’s a major shift that comes with profound security implications. Some 87% of companies have suffered an incident with a third party supplier that disrupted their operations, according to Deloitte.⁴ To do their work, gig workers and other contractors often require remote access to sensitive corporate resources. Yet many companies don’t apply the same security principles to third parties as they do to internal employees. These unknowns make gig and contract workers a big risk when it comes to your systems, files and data.

The problem isn’t just dishonest or disgruntled workers. Not every insider is malicious. According to Ponemon, 62% of insider threats are initiated by negligent employees or contractors.⁵ That makes insider risk a unique challenge.

A new set of principles should apply to everyone in the modern gig economy workforce. The logic of perimeter-based security no longer works. That’s because traditional network boundaries have been replaced by a dynamic new “people perimeter.”

This e-book shows you how to mitigate insider risk in this new work reality by:

- Understanding department-specific risks of third-party work
- Following best practices for proactive security
- Gaining visibility into both people and data for contextual awareness

² Karen Gilchrist (CNBC). “The pandemic has boosted freelance work — and hiring for these jobs is booming.” July 2020.
87% of companies have experienced an incident with a third-party worker that disrupted their operations. 

Q: Who is a Third-Party Worker?  
A: Anyone who is not an employee, including:

- Contractors
- Consultants
- Service Providers
- Supply Chain Partners

---

\(^7\) Deloitte. "Third-party risk is becoming a first priority challenge."
SECTION 1

Contractor Insider Risk in the News

Are you sure you trust the contract IT team?

Industry
Healthcare

Insider Risk Categories
Accidental/Negligent, Third-Party,
Data Exfiltration, Poor Security Hygiene

Cost to Business
$250,000 for SingHealth and $750,000 for responsible IT firm

The Problem
An IT agency hired by Singapore’s SingHealth failed to follow security best practices and ignored warning signs. This lapse led to a data breach that exposed the records of 1.5 million patients.

Lessons Learned:
1. SingHealth’s contractor neglected Singapore’s stringent regulatory requirements for privacy and security via the Personal Data Protection Act.
2. Insider threats can also originate with third parties, including IT vendors. Insider threat monitoring must cover all insiders.
3. A robust combination of insider threat technology, security awareness training, and responsible systems management is required for a complete security strategy.
SECTION 2

Contract Work: Where are the Security Risks?

Third-party or contract workers help companies add specialized talent without the overhead costs of salaries and benefits.

Here are some examples of how various business departments use third-party contractors—and the risks that may come with them. (The risk can vary according to level of access granted.)

<table>
<thead>
<tr>
<th>Department</th>
<th>Examples of Third-Party Work</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT</td>
<td>• Software developers</td>
<td>• Abuse of privileged access / admin credentials</td>
</tr>
<tr>
<td></td>
<td>• QA testers</td>
<td>• Negligence in setting up systems (such as database configuration management)</td>
</tr>
<tr>
<td></td>
<td>• Application configuration/customization</td>
<td>• IP theft</td>
</tr>
<tr>
<td></td>
<td>• Database administrators</td>
<td>• Data loss</td>
</tr>
<tr>
<td></td>
<td>• Employee tech support</td>
<td>• Data exfiltration to competitors</td>
</tr>
<tr>
<td></td>
<td>• Managed software or service providers</td>
<td></td>
</tr>
<tr>
<td>HR</td>
<td>• Recruiters</td>
<td>• Loss of sensitive data, including personally identifiable information (PII)</td>
</tr>
<tr>
<td></td>
<td>• Benefits administrators and software solutions</td>
<td>• Loss of company-confidential information (such as compensation records, culture incidents and more)</td>
</tr>
<tr>
<td></td>
<td>• Company culture analysts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Employee onboarding and offboarding solutions</td>
<td></td>
</tr>
<tr>
<td>Customer Service</td>
<td>• Call-center representatives</td>
<td>• Loss of customers’ PII or assets</td>
</tr>
<tr>
<td></td>
<td>• Content moderators</td>
<td>• Company data loss</td>
</tr>
<tr>
<td></td>
<td>• Translation services</td>
<td>• Abuse of privileged access</td>
</tr>
<tr>
<td></td>
<td>• Chatbots / customer service software</td>
<td>• Negligence with account credentials</td>
</tr>
</tbody>
</table>
### Department | Examples of Third-Party Work | Risks
--- | --- | ---
**Marketing** | Strategists for • Branding • Content • Public Relations • Design • Demand Generation | • Loss of sensitive corporate data • Loss of forward-looking data or plans • Data exfiltration to competitors • Negligence with cloud services or remote accounts

**Sales** | • Sales representatives • Lead-generation services • Prospecting • Account-based marketing • Sales lead databases and other software providers | • Data exfiltration to competitors • Loss of customer data or PII • IP theft • Negligence with cloud services or remote accounts

**Legal Services** | • Document and contract drafting/review • Legal research • IP work • Corporate counsel • Litigation support | • IP theft • Sensitive data loss • Abuse of privileged access

---

**Risky behaviors common to the contract workforce include:**

- Downloading files during irregular hours
- Installing unauthorized software
- Logging on from unusual endpoints
- Sharing account credentials
- Leaving credentials unprotected
- Sharing files with unauthorized users
SECTION 3

Vendor Insider Risk in the News

A newspaper finds itself in the headlines — and not in a good way.

**Industry**
Media and Communications

**Insider Risk Categories**
Third Party, Accidental/Negligent, Data Loss

**The Problem**
French newspaper Le Figaro’s accidental data leak — caused by a third-party hosting firm’s poor security hygiene — exposed 7.4 billion records.

**Lessons Learned:**
1. Third-party vendors must meet strict risk assessments before they are used to store or traffic valuable information about users.
2. Attacks often morph from data theft to more complex and dangerous attacks that target internal systems, so having early warning systems in place is key.
3. Database leaks are one of the most common insider threat types, so make sure yours are properly configured and that monitoring is in place to detect leaks.
Best Practices for Decreasing Risk in the Contract Workforce

Working with third parties doesn’t have to be risky if you employ the proper monitoring, alerting, and contextual intelligence.

Use this checklist to proactively address security with your third-party contractors and processes.

Access Rights
- Use the principle of least privilege. Enable access only to the accounts or systems third-party workers need
- Require strong passwords
- Require multi-factor authentication
- Use temporary or rotating admin credentials where possible

Onboarding
- Include NDAs or other sensitive data-handling agreements in contracts
- Review cybersecurity policies with all incoming workers
- Ensure that teams are collaborating with sanctioned cloud software
- Share sensitive onboarding information only with people who need to see it

Security Awareness Training
- Implement quarterly or biannual training on phishing and social engineering to prevent credential theft
- Train third-party workers on basic account practices and sharing best practices
- Test security knowledge retention with industry-appropriate attack simulations or quizzes
- Arm third-party workers with knowledge of how to recognize and report potential security issues
- Work with internal employees on reinforcing security policies with contractors

Offboarding
- Turn off access to accounts or systems when a third-party worker departs
- Change passwords for sensitive accounts
- Revoke access to sensitive documents
SECTION 5

Gaining Visibility Into People and Data

In today's dynamic economy, many more companies employ third-party workers. Yet security teams may not have the resources to deal with a distributed workforce.

What's the best way to manage the increased risks?

Restrictive cybersecurity policies aren’t the answer. Hybrid teams of employees and contractors need to access cloud-based solutions and other critical systems to do their jobs effectively. Too many restrictions can make people work around the rules. This can lead to even greater risks.

Instead, security teams should focus on building a comprehensive insider threat management program (ITMP). This should cover people, processes and technology. Many of the people and process recommendations above can proactively protect organizations from risk. From a technology perspective, organizations need visibility into third-party user and data activity. This approach helps security teams:

- Understand the context around a user’s motives
- See where the data is moving and why
- Distil valid signals from noise within security alerts

This approach helps security teams: [additional details]
CONCLUSION AND RECOMMENDATIONS

A modern workforce calls for a modern approach to managing insider risk. The gig economy and the contract workforce aren’t going away anytime soon. Depending on the department and the contractor’s level of access, insider threat risks can vary greatly.

Organizations can adapt to new risks by putting people at the center of their security strategy and investing in technology that provides full context.

5 Key Takeaways

1. Share an easy-to-understand security policy with third-party workers, including all gig, contract, and freelance workers

2. Work with internal employees to reinforce the policy with third-party workers

3. Empower third-party workers with security awareness training

4. Ensure that teams are collaborating using only sanctioned software

5. Use technology that provides context around third-party user activity and data movement.
About Proofpoint

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. Proofpoint.com

Learn More

For more information, visit proofpoint.com.