Imperfect People, Vulnerable Applications
Executive Summary

In a business environment increasingly dictated by software, building secure applications is critical. The release of compromised applications has hit the headlines in recent months with attacks such as Sunburst. However, organizations have yet to understand how to solve the underlying people issues allowing this to happen.

This report explores the human elements contributing to cyber risk in the Software Development Lifecycle (SDLC). It researched both development and security teams at large organizations to outline the scale of the problem on both sides and highlight the three specific issues causing it.

KEY TAKEAWAYS

The following are the key takeaways from this research:

• Developers knowingly release a significant number of vulnerable applications
  The vast majority of developers at large organizations—senior people in particular—choose to push live applications they know to be insecure.

• Security teams have little faith in the Software Development Lifecycle (SDLC)
  Only a minority of security teams believe their application build environment could withstand an attack similar to SolarWinds, with confidence low in application security as a whole.

• Overworked and under-resourced teams struggle to shift left
  Security and development teams do not have sufficient time and resources to support the necessary “shift left,” address prioritized vulnerabilities, or even work together effectively on the development of secure applications.

• A hazardous disconnect exists between front-line developers and their managers
  Many front-line developers do not see security as their responsibility. Their senior managers disagree but are clearly failing to build a culture of ownership around security.

• Information sharing and training lags behind a dynamic attack environment
  Security teams feel their understanding of the latest vulnerabilities and application attacks is lacking, as is that of development teams. Training is delivered too infrequently to keep pace with a dynamic threat environment.

ABOUT THIS WHITE PAPER

Data is drawn from the survey undertaken specifically for this white paper. We surveyed 260 people in application development and security roles in the United States and the United Kingdom at organizations with an average of 14,651 employees.
Security Risks in the SDLC

Our survey questioned application developers and security professionals to discern the human elements at play which create cyber risk in the Software Development Lifecycle (SDLC). The findings revealed significant issues.

DELIBERATE RELEASE OF VULNERABLE APPLICATIONS

A worrying majority of the development teams at large organizations we surveyed are knowingly releasing vulnerable applications with insecure code (81%). For the developer respondents as a single group, more than half are releasing insecure code “sometimes” or “often.” Senior development engineers—with the roles of Head of DevOps and Development Manager who have overall responsibility for the SDLC—are more than twice as likely as front-line development teams to commit insecure code “often.” With vulnerabilities forming one of the primary routes of ingress for attackers, this underlines a widespread issue for security teams.

See Figure 1.

Figure 1

Known Release of Insecure Code
Percentage of respondents (developer respondents only)

<table>
<thead>
<tr>
<th>Role</th>
<th>Never</th>
<th>Rarely</th>
<th>Sometimes</th>
<th>Often</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined</td>
<td>19%</td>
<td>27%</td>
<td>35%</td>
<td>19%</td>
</tr>
<tr>
<td>Head of DevOps</td>
<td>20%</td>
<td>26%</td>
<td>35%</td>
<td>20%</td>
</tr>
<tr>
<td>Development Manager</td>
<td>18%</td>
<td>26%</td>
<td>36%</td>
<td>20%</td>
</tr>
<tr>
<td>DevOps Developer</td>
<td>27%</td>
<td>36%</td>
<td>27%</td>
<td>9%</td>
</tr>
</tbody>
</table>

Source: Osterman Research (2021)

Development teams at large organizations are knowingly releasing vulnerable applications with insecure code.
INSECURE BUILD ENVIRONMENTS

Less than half of the security professionals in our research believe their application build environment is secure enough to withstand a dedicated attacker (44%). This exact issue was the underlying cause of the recent high-profile SolarWinds attack and points towards either a lack of awareness, skewed priorities, or inefficient operations in the SDLC. By role, front-line security teams were much less likely to consider the build environment secure than senior security staff. See Figure 2.

Figure 2
Build Environment is Sufficiently Secure—Security Professionals
Percentage of respondents (security respondents only)

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined</td>
<td>44%</td>
</tr>
<tr>
<td>CISO</td>
<td>50%</td>
</tr>
<tr>
<td>Director of security</td>
<td>48%</td>
</tr>
<tr>
<td>Security practitioner</td>
<td>31%</td>
</tr>
</tbody>
</table>

Source: Osterman Research (2021)

The number of development professionals who believe their build environment is secure enough is higher than security professionals, although the same variation exists between senior development engineers and front-line development staff. See Figure 3.

Figure 3
Build Environment is Sufficiently Secure—Developers
Percentage of respondents (developer respondents only)

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined</td>
<td>61%</td>
</tr>
<tr>
<td>Head of DevOps</td>
<td>63%</td>
</tr>
<tr>
<td>Development Manager</td>
<td>61%</td>
</tr>
<tr>
<td>Developer on DevOps Team</td>
<td>55%</td>
</tr>
</tbody>
</table>

Source: Osterman Research (2021)

For both groups, the low numbers indicate a state of unpreparedness and a major target for attackers across the board, especially with the tendency for copycat attacks linked to SolarWinds. With such vulnerabilities being notoriously difficult to detect and having a long dwell time, this points towards a potentially long-term issue.
LOW CAPABILITY TO DEVELOP SECURE APPLICATIONS

In general, only 56% of the security professionals in our research expressed confidence that the development and engineering teams at their organization could develop secure applications. By role, CISOs had the lowest level of confidence in comparison to the other two groupings of security professionals. See Figure 4.

Figure 4
The Ability of Development/Engineering Teams to Develop Secure Applications
Percentage of respondents (security respondents only)

Source: Osterman Research (2021)

Examples of this low level of confidence were expressed across multiple rating questions, such as:

- **Security teams on withstanding targeted attacks**
  Only 54% of CISOs believe the applications developed by their organization would withstand a targeted attack. Front-line security teams express even less confidence, at only 44% of respondents.

- **Security teams on withstanding low-level attacks**
  Only 63% of CISOs believe the applications developed by their organization could withstand a low-level attack. The confidence of front-line security teams was lower, at 50% of respondents.

DevOps teams expressed a higher level of confidence in their security capabilities compared to the security respondents. For instance:

- **Developers on withstanding targeted attacks**
  66% of respondents felt confident that the applications developed by their organization could withstand a targeted attack. This confidence rating is almost 30% higher than the rating given by security respondents.

- **Developers on withstanding low-level attacks**
  69% of respondents felt confident their applications could withstand a low-level attack, a confidence rating 13% higher than the security respondents.
Why the Gap?

Treating security as a bolt-on to software application development projects has been implicated in the release of insecure code. Many believe a secure SDLC is one which is cognizant of the multitude of complex “softer” human elements at play which manifest in code, ranging from organizational culture at the broad end of the spectrum to each developer’s training at the other.

Instead of writing yet another piece pointing to a difficult dynamic between security and development teams, we wanted to push deeper in this research to understand the factors contributing to this gap. We observed three main themes, which if improved, would have a beneficial impact on the human elements currently increasing risk in the SDLC.

A DESIRE TO SHIFT LEFT—BUT NOT ENOUGH RESOURCE

The research underlined an aspiration to achieve the shift left in order to build security into the SDLC earlier on. Security teams are keener than their developer counterparts, but in both groups, the prevailing opinion is that the earlier security is considered, the lower risk the application. See Figure 6.

Figure 5
When Security Should First Be Considered in the SDLC
Percentage of respondents

<table>
<thead>
<tr>
<th>When Security Should First Be Considered in the SDLC</th>
<th>Developer</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements analysis</td>
<td>29%</td>
<td>36%</td>
</tr>
<tr>
<td>Planning</td>
<td>25%</td>
<td>31%</td>
</tr>
<tr>
<td>Application design</td>
<td>14%</td>
<td>15%</td>
</tr>
<tr>
<td>Application development</td>
<td>9%</td>
<td>16%</td>
</tr>
<tr>
<td>Testing</td>
<td>9%</td>
<td>7%</td>
</tr>
<tr>
<td>Deployment</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Maintenance</td>
<td>1%</td>
<td>1%</td>
</tr>
</tbody>
</table>

Source: Osterman Research (2021)

However, this desire to shift left is currently hindered by security and development teams being constrained by a lack of time and resources. Data points in the analysis which highlight this gap include:

- **Insufficient time and resourcing to shift left**
  Only 39% of security respondents said their team had sufficient time and resources to support the shift left.
- **Not enough time and resources to address prioritized vulnerabilities**
  Only half of security respondents agreed they had sufficient time and resources to address prioritized vulnerabilities in applications. In other words, the ability to address current and known security issues is significantly under-resourced.

- **No time to work with development team**
  Only 44% of security respondents said they had the time necessary to help the development team secure applications.

When these data points are broken out by role, the first and second were more acutely felt by front-line security teams than senior security professionals. It would appear the latter believe something to be true that front-line staff do not experience in practice. See Figure 6.

Figure 6
**Lack of Time and Resources for Security Team**
Percentage of respondents (security respondents only)

![Chart showing lack of time and resources for security teams](source: Osterman Research (2021))

Developers in general were more likely than their security counterparts to say they had sufficient time and resources to complete their tasks. This would appear to indicate that of the two, security teams are more stretched to perform with current resourcing levels. See Figure 7.

Figure 7
**Sufficiency of Time and Resources to Complete Various Tasks**
Percentage of respondents

![Chart showing sufficiency of time and resources](source: Osterman Research (2021))

*Front-line security teams lack time and resourcing to support shift left.*
GAP BETWEEN SENIOR AND FRONT-LINE TEAMS

There was a noticeable gap in the ratings provided by respondents in senior roles and those on front-line teams. This was true in both the security and developer cohorts. This is to be expected as responsibilities differ, but the gaps highlight that those building the applications themselves have the lowest level of personal ownership of security, as well as a poor understanding of the latest application security threats. See Figure 8.

Figure 8
Gaps in Security—Developers
Percentage of respondents (developer respondents only)

![Gaps in Security Chart]

Source: Osterman Research (2021)

For the developer respondents, specific data points included:

- **Poor ownership of security by front-line developers**
  Only 27% of front-line developers view the security of applications as a critical part of their responsibilities. By comparison, 80% of respondents in both of the senior roles took this view. There is a problem when those at the coalface of development feel such low ownership for security.

- **Security should not be part of the SDLC**
  Only 55% of front-line developers agreed that security considerations should be part of the SDLC, compared with 66% of respondents in the development manager role and 85% in the Head of DevOps role. This speaks to the need for greater awareness of security in the SDLC through education and training, along with better tooling and closer integration with security teams to do so.

- **Understanding new application security threats**
  While 80% of respondents in the Head of DevOps role claimed to understand the latest threats to application security, only 64% of those actually writing the code said the same. What is understood by senior professionals is not effectively cascading to the front line.
• **Lack of information on the front line**
  In comparison to those in the Head of DevOps role, roughly half as many front-line developers agreed they had timely access to security information to help them build applications securely (63% and 36% respectively). Development managers were at the midway point (49%). As with all previous data points, this is the inverse of what should be at play to ensure the people building apps can do so securely.

The security respondents likewise evinced a similar role gap, for example:

• **Not my responsibility**
  Only half of front-line security staff view safeguarding applications as a critical part of their responsibilities, compared to 73% for security directors and 76% for CISOs.

• **Not my job**
  Senior security professionals see themselves playing a more active role in securing applications than front-line security staff: 69% of CISOs and 76% of security directors, but only 56% of security practitioners.

• **Not my toolkit**
  Fewer front-line security staff have access to threat intelligence to improve application security than senior professionals: 50% of security practitioners, 61% of managers, and 70% of CISOs.

See Figure 9.

**Figure 9**
Gaps in Security—Security Team
Percentage of respondents (security respondents only)

Gaps of this nature can stop the integration of security principles in the earliest stages of the SDLC—which acts against the shift left movement.

*Front-line security professionals are more likely than senior security staff to see security as not their responsibility or job.*
OUTDATED INFORMATION SHARING, EDUCATION, AND TRAINING

The techniques and approaches currently used for sharing information, education, and training are outdated and insufficient. These slow legacy approaches are not embedding the knowledge required to match a fast-paced threat landscape and dynamic technology fundamentals. The survey results illustrate a sad state of affairs:

- **Insufficient understanding of threats**
  Only 54% of the security respondents believe developers understand the latest threats to application security. This drops to 44% for front-line security practitioners. Less than half of security respondents say they have the time necessary to learn how to secure applications (47%), and therefore it is unsurprising that 40% of security respondents say they lack a comprehensive understanding of the SDLC.

- **Slow cadence of information from security teams**
  Three quarters of development teams receive threat information weekly or less frequently from the security team, with 25% of development teams on a monthly or slower cadence. See Figure 10.

  ![Figure 10](image)

  **Figure 10**
  Frequency of Receiving Threat Information
  Percentage of respondents (developer respondents only)

  Source: Osterman Research (2021)

- **Classroom training still used**
  Half of organizations rely on classroom-based approaches for training developers on application security. For a modern remote workforce, especially considering the global pandemic over the past year, this is close to half of all organizations with an irrelevant training structure for securing the SDLC.

- **Slow cadence of security training**
  Half of security teams offer training on application security to engineering and development teams on a quarterly or less frequent cadence. See Figure 11.

Legacy approaches to information sharing, education, and training are not embedding the knowledge required to match a fast-paced threat landscape.
• **Ineffective onboarding**
  Half of the new employees joining an organization are not provided with effective training on application security, according to the security respondents to the survey.

The gap between front-line and senior developers was also evident in terms of education and training (see Figure 12). For example:

• **Lack of learning time for developers**
  Only 45% of front-line developers say they are given the time necessary to learn how to create secure applications, compared with 59% for development managers and 65% for respondents in the Head of DevOps role.

• **Poor understanding of the latest threats**
  Fewer front-line developers (64%) say they understand the latest threats to application security than respondents in the two senior roles (68% and 80% for the manager and head roles respectively).

• **Low efficacy on learning from mistakes**
  Front-line developers were half as likely as Head of DevOps respondents to say they learn from mistakes to develop more secure applications—36% for developers and 69% and 72% for respondents in the manager and head roles respectively. Poor efficacy for after-the-event learning dooms development teams to repeating the same mistakes.
Summary
It is gratifying to see an aspiration to achieve the shift left and build security into the SDLC earlier on. However, nothing will shift until urgent action is taken to address the three main themes explored in this research and thus translate the aspiration into a culturally embedded approach.
About Immersive Labs

Immersive Labs is empowering organizations to equip, exercise, and evidence human cyber capabilities. We provide metrics that give security leaders insight into human cyber skills and readiness levels across their organization and improve these through dynamic labs and crisis scenarios which track the threat landscape. Immersive Labs is backed by Goldman Sachs and Summit Partners and our customers include some of the largest companies in financial services, healthcare, and government, amongst others.

For more information on Immersive Labs’ offering, please visit www.immersivelabs.com