Investigation or Exasperation? The State of Security Operations
We’re Under Attack (But by How Much?)

On average, 62% of firms are being attacked at least weekly, with a fifth attacked daily and 10% hourly or continuously.

Big companies (with more than 1,000 employees) suffer more attacks, with 68% of firms being hit at least weekly. Smaller firms seem less vulnerable, or do they lack the visibility to detect the attacks?

Bigger firms are also seeing bigger rises in attack rate from a year ago. Perhaps they are getting better at detection, or maybe they present a more attractive target for hackers.

Source: IDC Custom Survey, March 2017, n = 600
We’re Overwhelmed

Describe your ability to cope with the number of security incidents.

- 0% We are completely overwhelmed
- 5% We are constantly firefighting
- 28% We usually cope but it’s sometimes a struggle
- 41% We cope more often than not, with a few stressful moments
- 27% We cope quite comfortably

Two-thirds of enterprises experience a security attack at least once a week, 30% of firms are being attacked at least daily and 10% suffer hourly or continuous attacks.

Firms experience an average of 40 actionable incidents per week. Some of these will translate into genuine attacks but others require investigation in order to determine that they are benign.

But only a quarter (27%) think they are coping comfortably with this workload, and a third describe themselves as “struggling” or “constantly firefighting.”

How many actionable* security-relevant alerts or incidents a week do you typically receive across all of IT?

- None: 12%
- Fewer than 10: 37%
- Between 10 to 40: 31%
- Between 50 to 100: 14%
- Between 100 and 499: 6%
- Between 500 and 999: 0%
- 1,000 or more: 0%

Source: IDC Custom Survey, March 2017, n = 600

Actionable incident /ˈɑkʃ(ə)nəb(ə)l ˈɪnsɪd(ə)nt/
noun
A security event or alert requiring intervention in order to investigate the reported issue, escalate it, classify it as an attack, or otherwise resolve it to closure.
We’re Failing to Operationalize and Prioritize Security Incidents

How do you classify the severity of incidents?

- **3%**: We have no way to classify the severity of incidents
- **24%**: All incidents are initially treated the same
- **26%**: We have a system of prioritization based primarily on the attributes of the attack
- **34%**: We have a system of prioritization based primarily on the criticality of the system, user, or service under attack
- **13%**: All incidents are automatically assigned priorities by our incident management platform

A quarter (27%) of firms don’t classify the severity of incident at all and another quarter (26%) only classify based on the attributes of the attack (but not the system, service, or user under attack).

Only 47% of firms gather information about an incident that allows them to take appropriate or decisive action (see graph on next page).

Source: IDC Custom Survey, March 2017, n = 600
Are Companies Making Up Response Actions as They Go Along?

81% of firms don’t have defined run books and 75% don’t have a managed incident response plan.

56% of organizations only gather information sufficient to take reasonable action or to look in the general direction. Only 21% gather information that enables a decisive action. And 40% have only a broad incident response plan in place.

Yet more than half of organizations experience 10 or more security incidents or alerts per week. How are they responding to these incidents? There is often no detailed plan in place, and rarely a technology platform that supports it.

Which statement best describes your organization’s response to incident alerts?

- 2% We have no defined responses to incidents
- 14% We have a managed incident response plan
- 25% We have an incident response management platform that automates the process
- 19% We have a detailed run book of incident types
- 40% We have a broad incident response
- 0% We generally have insufficient information in order to take action
- 12% We gather information that points us in a general direction
- 24% We gather sufficient information that directs us toward an appropriate action
- 20% We gather detailed information that allows us to take decisive action

Source: IDC Custom Survey, March 2017, n = 600
Incidents Are Too Time Consuming

How many people are involved in an incident?

- 1: 17%
- 2 or 3: 12%
- 4 or 5: 3%
- 6 to 9: 1%
- 10+: 69%

Do the math.

- Two people doing two hours' work per incident, 10 incidents per week = an average of one fulltime resource on incident response.
- Most incidents require teamwork: over 80% of incidents involve two or more people.
- This is the truth behind resource limitations: we're too busy on response (whether planned or emergency).

What's the effort required in dealing with an incident?

- < 1h: 13%
- 1-2h: 34%
- 2-4h: 36%
- 4-8h: 12%
- 9-12h: 3%
- 13-20h: 4%

Source: IDC Custom Survey, March 2017, n = 600
# Why Can’t We Just Have More…

## Resources/Focus/Technology/People/Budget/Time, etc., etc.

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources are too busy on routine operations (e.g., incident investigation)</td>
<td>53%</td>
</tr>
<tr>
<td>Juggling conflicting priorities</td>
<td>44%</td>
</tr>
<tr>
<td>Not enough integration into the IT infrastructure teams</td>
<td>35%</td>
</tr>
<tr>
<td>Budget constraints</td>
<td>32%</td>
</tr>
<tr>
<td>High level of demand for new business services</td>
<td>28%</td>
</tr>
<tr>
<td>Lack of insight into security-sensitive activities</td>
<td>27%</td>
</tr>
<tr>
<td>Skill shortages</td>
<td>26%</td>
</tr>
<tr>
<td>Security team spends time maintaining and managing security tools rather than performing security investigations</td>
<td>23%</td>
</tr>
<tr>
<td>Fragmentation or lack of integration of security product portfolio</td>
<td>19%</td>
</tr>
<tr>
<td>Competing with cloud resources used/shadow IT</td>
<td>14%</td>
</tr>
</tbody>
</table>

Source: IDC Custom Survey, March 2017, n = 600

- **Main limitation in U.S. and in larger companies (1,000+ employees)**
- **Top inhibitor in the U.K. and the Netherlands**
- **Main inhibitor in France, Germany, and Sweden, and in companies with 500–999 employees**

**What is limiting your ability to improve your IT security capabilities?**
When do you invest in security?

- 73%: As part of our strategic investment plans in security.
- 72%: When we have discovered a vulnerability ourselves.
- 62%: When a vulnerability has been disclosed to us by an outside party or when we are made aware of an emerging new threat type or sector.
- 55%: When we have conducted a penetration test that reveals weaknesses as part of an overall program to improve security provision.
- 53%: When you have a serious breach.

Companies need more of everything. Routine ops and incident investigation are by far the biggest drag on efficiency.

And while 73% of firms plan security spend according to their strategy, the same number (72%) also spend reactively when a vulnerability is discovered.

The list of limiting factors is long, and most firms still tend to spend on security in a crisis. How do we break this cycle, increasing efficiency while spending in line with plan?

Source: IDC Custom Survey, March 2017, n = 600
Are We Communicating the Real Risk Effectively to Senior Management?

When do you report an incident to the board?

- Most firms surface a breach to the board when there's no hiding it any longer: a sensitive data breach, or customer data, or a mandated notification to a regulator.
- Only 35% of firms have breach reporting to the board built in to their defined incident response processes.
- Boards are unlikely to support process and efficiency improvements if they don’t understand the volume, scale and regularity of attacks and time spent investigating incidents.

- When a data breach relates to sensitive data (aka special categories of data): 66%
- When customer data has been compromised: 57%
- When required to do so by law or by a regulator: 52%
- Immediately on classification as a severe or impactful breach: 52%
- When data is discovered to have been exfiltrated: 38%
- Immediately on discovery/detection of security breach: 37%
- This is built in to our internal incident response process: 35%
- When the breach becomes public: 26%
- We don’t report breaches to the board: 2%

Source: IDC Custom Survey, March 2017, n = 600
Threat Concerns Drive Investment, but Compliance Looms Large

Nothing drives investment like the thought of a threat. This makes sense: it’s the purpose of security to identify — and defeat — threats.

But compliance concerns are a close second. Importantly, technical standards are compounded by less prescriptive, risk-based requirements, like GDPR. These drive budget because they tap into business (as opposed to security threat) risk: the consequence of non-compliance for a business may be greater than a security breach.

To what extent are the following driving your investments in IT security?

- Our understanding of the threat landscape: 3.82
- Compliance requirements such as GDPR, ISO2700x, or PCI DSS: 3.65
- A recent breach or compromise: 3.50
- Business initiatives such as digital transformation and IoT: 3.18
- Inputs from third-party providers and government sources: 3.06
- A need to increase our internal resources and skills space: 2.96
- Adoption of cloud services: 2.92
- Cyber insurance requirements: 2.80
- A strategic decision to outsource some or all of our security provision: 2.51

Mean rating 1: Not at all – 5: Very significant
Incident Response Lowers Costs, but Also Protects the Brand

Better incident response is aimed at improving the overall operational cost of security, more than simply reducing the cost of IR itself. The benefits are expected to be seen across the whole security operation.

Brand reputation is the other big gainer. An incident is the moment of truth for organizations, the point at which they must demonstrate compliant processes in IR, forensics, record keeping, and so on. Regulators do not expect zero breaches. But they do expect organizations to detect breaches early, to be able to determine the impact quickly, and to effect remediation efficiently. The ability to recover from a breach preserves reputation.

Please indicate which of the following KPIs have improved the most or could improve the most as a result of adopting incident response capabilities.

- Lower operational cost of security: 56%
- Brand reputation protection: 49%
- Secure adoption of new technologies (such as Cloud and IoT): 47%
- Demonstrable improvement in compliance posture: 46%
- Lower cost of security incident response: 39%
- Enablement of digital transformation programs: 38%
- Reduction in cyber insurance premiums: 24%

Source: IDC Custom Survey, March 2017, n = 600
Vertical Views

How many actionable security-relevant alerts or incidents a week do you typically receive across all of IT?

Source: IDC Custom Survey, March 2017, n = 600

Average actionable incidents

124
Telco

77
Finance

72
Retail & Wholesale

Telco, finance and retail and wholesale are seeing the most incidents per week...

How long does it typically take to resolve a security incident from detection to resolution?

Manufacturing and non-IT professional services have the biggest struggle with incident volume.

What statement best describes your ability to cope with the number of security incidents raised?

- We cope quite comfortably
- We cope more often than not, with a few stressful moments
- We usually cope but it’s sometimes a struggle
- We are completely overwhelmed

Manufacturing, transport and distribution, and retail and wholesale spend the longest time resolving an incident.

Source: IDC Custom Survey, March 2017, n = 600
Essential Guidance

Handling security incidents is a time-consuming activity. But most organizations have poor processes to manage the substantial effort. On average, organizations in our survey employ one FTE just on incident investigation, yet it is extremely unlikely that this is recognized, budgeted for, and managed. Most organizations do not have a dedicated incident investigation team.

Not only is security investigation time consuming, but organizations are also failing to effectively protect themselves. Despite the vast quantities of data being gathered, only 21% gather information on incidents that enables a decisive action.

The biggest time sink is routine operations such as incident investigation: this is constraining improvements in security.

Most incidents require teamwork: over 80% of incidents involve two or more people. This suggests that organizations need a platform where they can collaborate during incident investigation.

Rates of attack show no signs of abating, and 45% of firms are experiencing a rise in the number of incidents. Most firms are overwhelmed with security issues, yet are consumed by routine tasks that divert attention away from efficient incident investigation.

Source: IDC Custom Survey, March 2017, n = 600
Call to Action

How aware are you of your organization's security operation in terms of time spent on incident investigation? Do you know what it's costing you in budget and time?

Do you want to find out how you compare to your peers? Determine your response readiness by using our free and easy-to-use self-assessment tool.
Methodology

IDC’s 2017 Security Survey

In April 2017, IDC conducted a survey of 600 global organizations with over 500 employees to understand the current readiness of security, to find out where organizations are focusing their security efforts, and what is driving the need for security.
About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company. Further information is available on our websites at www.idc.com

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2017 IDC. Reproduction without written permission is completely forbidden.