SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > Policy >

# Not Following Established Policy Tops List of Most Significant Threats to Information Protection

Created by the Security Executive Council

## The State of the Industry

This state of the industry report is being prepared by Kennesaw State University's Center for Information Security Education (CISE) partnering with the Security Executive Council (SEC). It will include survey results from the first in a bi-annual series of assessments of the threats to information protection. It is critical to collect this information given the high degree of change experienced in industry. Due to the large number of successful attacks against high value and high visibility targets, senior management is interested in this topic more than ever before. Knowing the landscape can be helpful in your internal decision making.

The data that will be included in the report and is included in this summary was collected from 267 respondents solicited from a pool of over 12,000 Information Technology / Information Security executives from January to April of 2015. The complete report, estimated to be ready for distribution in the Third Quarter of 2015, and available from SEC, will provide an aggregation from widely referenced trade and vendor reports. A preview of the novel survey results is presented following.

## Summary of the 2015 Survey

### Demographic Profile

Roughly 90% of respondents were from the USA. The largest single identified group of respondents was from the Public Sector: Government, Military and Education at ~36%,

with ~60% of responses were from the industrial and commercial sector. Almost half of respondents (~48%) were from organizations with 5000+ employees, and ~62% reported gross annual revenues of over $50 Million. About one-third (~32%) had organizational security budgets over $2.5M.

Almost two-thirds of respondents (~65%) indicated they were an 'Information Security Executive or Manager' and ~57% considered themselves to be the senior-most executive or manager responsible for information security within their organization. Over 82% of respondents reported 2 or fewer layers of management between their position and the top executive of the organization and fully half (50.0%) reported to the top IT exec (e.g. CIO).

Approximately 38% of respondents reported their organizations employed 1 to 5 full-time information security employees, with another ~17% employing 6-10. Almost half (~45%) reported no open positions while over one-third (~35%) indicated their organizations currently had 1 to 5 open positions. Around one-third (~32%) reporting no turnover in full-time infosec positions in the last few years, with approximately 26% reporting 1-5% turnover, and another 21% indicating 6-10%.

When asked to report on the current threats facing their organization, respondents identified these as the top five most significant 'general' threats:

1. Electronic Phishing/Spoofing attacks
2. Malware attacks
3. Loss of trust due to information loss.
4. Unintentional employee/insider mistakes
5. Software failures or errors due to unknown vulnerabilities in externally acquired software

Respondents indicated these as the top five most significant threats from internal sources:

1. Inability/unwillingness to follow established policy
2. Disclosure due to insufficient training
3. Unauthorized access or escalation of privileges
4. Unauthorized information collection/data sniffing
5. Theft of on-site organizational information assets

And these as the top five most significant threats from external sources:

1. Unauthorized information collection/data sniffing
2. Unauthorized access or escalation of privileges
3. Website defacement
4. Intentional damage or destruction of information assets
5. Theft of mobile/laptop/tablet and related/connected information assets

When asked to name specific technologies that posed a risk to the security of their organizations information assets, respondents chose these as their top five:

1. Cloud-based data storage
2. Cloud-based applications
3. Mobile technologies
4. "Bring Your Own" Devices (BYOD)

5. Social media

## Changes in Attack Patterns

Most respondents found a slight increase (38.5%) or about the same (36.9%) in the number of attacks from 2013 to 2014. Likewise, most respondents felt changes made by the organization had the effect of causing a slight decrease (30.4%) or no change (34.8%) in the number of attacks experienced by the organization. Organizational responses over recent years were perceived to have a slight decrease (31.3%) to no change (31.3%) in the impact of successful attacks experienced by the organization.

## Conclusion

We hope that this early look at some of the survey results has been useful and will assist you in your information protection role. Look for the complete report, available from SEC, later this year.

**Visit the Security Executive Council website for other resources in the Program Best Practices: Policy and Guidelines series.**

## About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com

Website: https://www.securityexecutivecouncil.com/