Top-to-bottom Cyber-Security Policy Needed

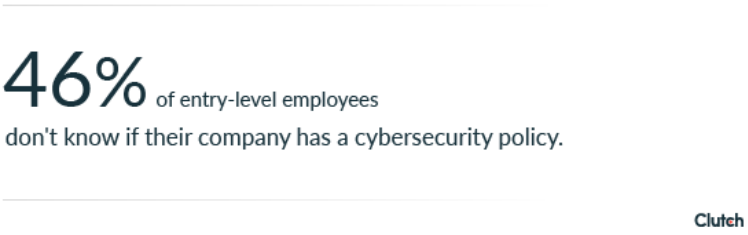
In the digital economy, almost all businesses depend on computers, smartphones and the Internet to function. Thus, most are now potential targets for cyber-criminals. Clearly, modern companies need an effective cyber-security policy.

Attacks continue to increase in number and severity because bad actors are getting rich from the market for stolen data. As will be shown, a lack of awareness among entry-level employees and the need for top leaders to get behind security policies leaves many companies dangerously exposed.

Entry-level Employees Unaware

According to the February 15, 2018, article, *Employee Awareness of IT Security Threats*, appearing on the business review site, clutch.co, just 52% of companies have adopted cyber-security policies. The article cites as its source a recent survey of 1,000 employees in various industries and across all company sizes and positions.

According to the survey, 28% of employees don't even know if their company has a cyber-security policy. That number grows to 46% among entry-level employees. To repeat, half of all companies surveyed don't have a cyber-security policy and almost half of all employees are not getting briefed on cyber-security when hired.



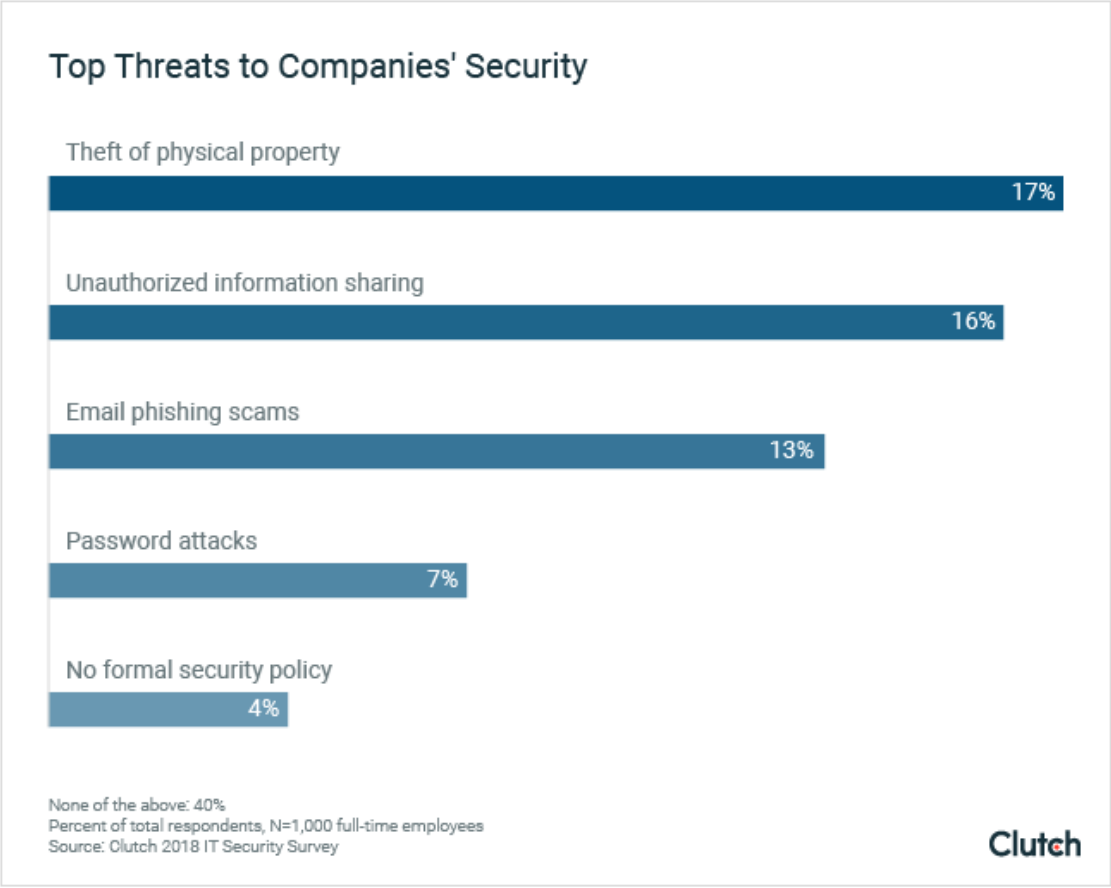
Surprisingly, an overwhelming 86% of entry-level employees surveyed don't know that the number of cyber-attacks and threats is likely to increase in the next year. Yet, they remain generally confident in their company's preparedness to handle threats.

> *"The latest brazen ransomware attacks are a sign of more to come. As long as someone is not prepared, the attacks will continue," related Jennifer Mazzanti, CEO of eMazzanti Technologies. "Organizations must act now to shore up their defenses because every business is already a target."*

Since unaware employees make easy targets for cyber-criminals' social engineering attacks, this lack of awareness increases the risk of suffering a breach.

Tangible Threats More Real

Curiously, the survey showed that employees rank burglary above anything related to IT services or cyber-security as the greatest threat to their companies.



One expert quoted says that the failure to identify cyber-security threats as dangerous relates to their tangibility.

> *"If you have experienced personal theft, or friends or relatives have experienced personal theft, then you become more aware," said Stephen Scott-Douglas, CIO of Ciklum, a global software engineering and solutions company. "The same applies to information security. There is something about experience that makes it real for people."*

Since cyber-security threats put data at risk rather than physical property, it's easier for employees to perceive them as impersonal. In addition, if company data is stolen rather than personal information, that perception is even more likely.

Cyber-Security Policy Drives Awareness

Cyber-security policies promote awareness among employees which leads to better preparation for cyber-security threats. According to the survey, employees at companies with cyber-security policies are more likely to:

- Feel prepared for IT security issues
- Think the number of IT security threats will increase over the next year
- Identify IT services concerns as the biggest threat to their company security

These attitudes decrease the likelihood that a company will suffer a security breach. Survey data showed that employees at companies with cyber-security policies understand that business practices involving data sharing and email are the most vulnerable.

Security policies also increase awareness of the cyber-threat landscape. Employees at these companies are more likely to say the number of threats will increase in the next year—a realistic assessment.

Security-first Mindset Starts at the Top

The commitment of company decision-makers to security directly impacts the security attitudes of employees. Commitment at the top is required for effective cyber-security throughout an organization, said Carl Mazzanti, co-founder and Vice President of eMazzanti Technologies, a New York City area IT security consultant and provider.

> *"If the CEO is not committed to it, an effective policy is unlikely," said Mazzanti. "Unfortunately, a recent security breach or loss has a way of motivating CEOs to implement a policy."*

Instead of a reactive policy, Mazzanti suggests a top-down security-first mindset as the first step in an effective cyber-defense.

Cyber-Security Policy Training at All Levels Needed

To improve cyber-security awareness among employees, companies need to require security training for all employees, including new hires. The lack of cyber-security training for new employees is a major cause of employee unawareness of security threats.

Understandably, companies are more likely to train higher-level employees who are considered higher security priorities. However, entry-level employees, who outnumber high-level employees, also pose a risk to the organization.

Companies should provide security training for all employees, irrespective of position. Company-wide training promotes cyber-security awareness, hence, stronger security at all levels of the organization.

The Weakest Link

No matter how strong a company's cyber-security technology may be, employees still manage to introduce threats into company networks by falling prey to phishing scams, giving away passwords and posting sensitive information on social media.

The 2017 IBM X-Force Threat Intelligence Index shows that data breaches involving email archives, intellectual property, and business documents all rose in 2016. It also shows that 85% of malicious email attachments were ransomware or ransomware downloaders.

> *According to the report, the use of spam email as an attack vector shows how important it is for organizations to improve their defenses against email attacks.*

To limit potential attacks and mitigate losses, every cyber-security policy should clearly communicate best practices for users. However, policies should be carefully crafted to minimize negative effects on productivity.

Leadership and Training the Key to Effective Cyber-Security Policy

As the survey quoted above shows, many employees, especially at the entry-level, lack awareness of company cyber-security policy and the trend of increasing IT security threats.

Despite these security awareness gaps, many employees are confident in their company's IT security preparedness, in part because they consider physical theft of company property more of a threat than risks that involve IT.

> *"The Equifax hack shows that cyber-criminals still see huge opportunities to profit from stolen customer data," stated Mazzanti. "Business owners must make customer data security a top priority or suffer similar losses."*

Finally, according to cyber-security experts, a lack of leadership from CEOs and business owners makes a cyber-security policy unlikely to succeed. Therefore, to avoid falling victim to increasing cyber-security attacks, CEOs and owners must drive cyber-security policies, carefully crafted policies that treat security as important for employees at all levels.