

Cybersecurity Awareness Month


October is Cybersecurity Awareness Month, a great time to educate your whole organization on the important role every employee in your organization can play in keeping your business safe. Take a look at a few key facts that you can share with every department.



Cybersecurity breaches could be very costly to your organization.

\$149,000 Average financial impact of a data breach for *SMBs* in North America.

\$1.6 million Average total financial impact of a data breach for large *enterprises* in North America.



Employees who are cybersavvy play an important role in keeping your organization safe.

\$113,000 Cost to *SMBs* of careless or uninformed employees.

\$1.24 million Cost to large *enterprises* of careless or uninformed employees.

\$98,000 Cost of inappropriate use of IT resource at *SMBs*.

\$1.06 million Cost of inappropriate use of IT resource at large *enterprises*.



Kaspersky Lab's Cybersecurity Awareness Services is a highly interactive and stimulating program that promotes engagement and a willingness to learn about cybersecurity awareness.

- Covers a wide range of cybersecurity issues
- Takes place in familiar environments
- Incorporates practical exercises and tools to measure employees' skills



Look outside your organization to your cloud providers and vendors. Are their systems secure?

\$115,000 Incidents at *SMBs* affecting third party cloud services.

\$1.13 million Incidents at large *enterprises* affecting third party cloud services.



Targeted attacks are very costly and affect organizations of all sizes.

\$140,000 Average financial impact of targeted attacks to *SMBs*.

\$1.23 million Average financial impact of targeted attacks to large *enterprises*.

What steps can you take to keep your organization secure?

The best place to start is by keeping your IT staff on top of current trends and risks and then implementing certain key policies, such as:

- ✓ Ensure that all users know and observe company security policies.
- ✓ Educate users about possible consequences of key threats, such as phishing, social engineering or malware sites.
- ✓ Employees should notify IT security staff about all incidents.
- ✓ Maintain control over user access rights and privileges. Any rights and privileges should be granted only when necessary.
- ✓ Record all rights and privileges granted to the users.
- ✓ Scan your systems for vulnerabilities and unused network services.
- ✓ Detect and analyze vulnerable network services and applications.
- ✓ Update vulnerable components and applications. If there is no update, vulnerable software should be restricted or banned.

To learn how you can get full protection for your business, call Kaspersky Lab at 866-563-3099 or email at corporatesales@kaspersky.com