

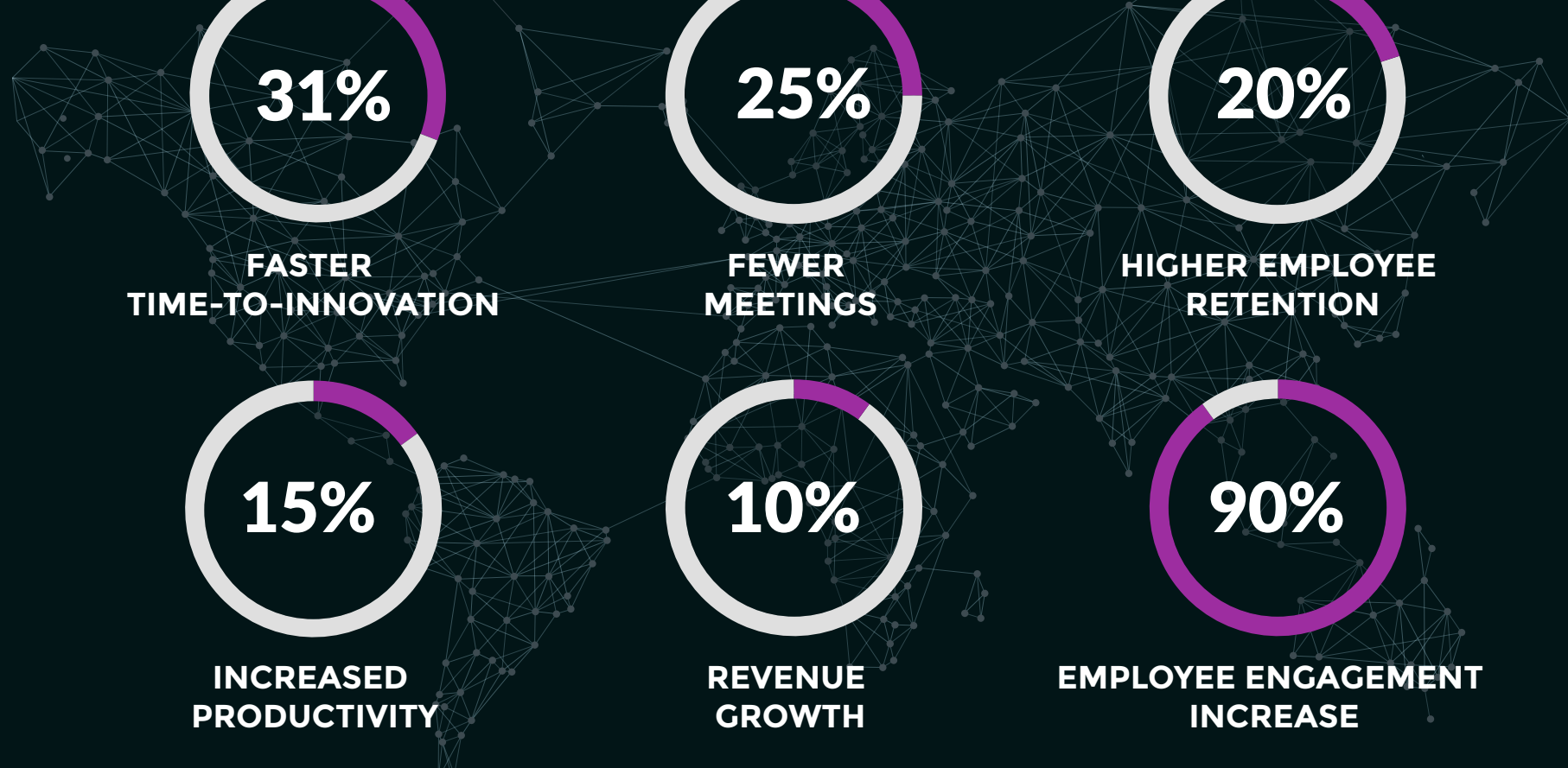
TOP 5

ENTERPRISE COLLABORATION SECURITY RISKS

The rise of Enterprise Social Networks (ESNs) and enterprise collaboration and messaging tools brings unprecedented collaboration opportunities to organizations that embrace them. But with new opportunities come inherent risks.

ESNs BRING UNPRECEDENTED OPPORTUNITY

ESNs help break down existing silos of information, people and processes and expedite innovation, productivity and output. Benefits include:¹



ESNs COME WITH INHERENT RISK

If ESNs are not properly secured and automatically monitored, risk to the organization is high — and fallout can be costly. The 5 most common risks are:

HR POLICY VIOLATIONS

Even Small HR Violations Can Lead to Huge PR Nightmares.

If not monitored and addressed, cases of harassment can go unreported and the violated employees simply leave — or worse, a lawsuit ensues.

In 2016:

91,503

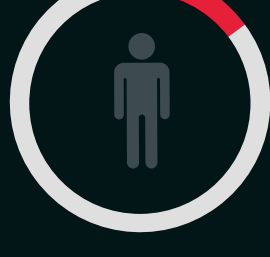
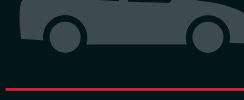
workplace discrimination charges were filed in the U.S.²

\$482 M

was secured for victims of discrimination.³

UBER

Uber has lost billions in sales and market capitalization due to its scandals that were well documented on the company's internal social collaboration platforms.⁵

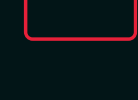


29% of women and 12% of men reported being sexually harassed in the workplace at some point in their career.⁴

DATA LEAKS

Intentional or Not, Data Leaks Can Be Costly.

Many companies don't realize that the security embedded in their collaboration tools may not be enough to properly protect them from one of the most common security risks — accidental or intentional data leaks.



40%

Data breaches increased by 40% in 2016.⁶



46%

46% of companies have suffered damage to their reputation due to a data breach.⁷



\$4 Million

The average cost of a single data breach in 2016 was \$4 million.⁸

1
100
1100001
011010010
101 10 0101
0101100001011
001110100 1
11001011100
101111

INSIDER THREATS

A Growing Threat from Within.

Today, insider threats have emerged as one of the biggest risks to corporate data — and ESNs have given employees and partners new and greater access to sensitive information.

80 Million

annual insider attacks each year.⁹

\$10+ Billion

estimated cost associated with insider threats.¹⁰

WHO ARE THE REAL THREATS?¹¹

31.5%

Malicious Insiders



45%

Outsiders

23.5%

Inadvertent Actors



77% of IT professionals said their employees leverage unsanctioned cloud-based solutions.¹²

REGULATORY COMPLIANCE

The Cost of Compliance is High, but the Cost of Non-compliance can be Crippling.

Compliance challenges are growing and changing all the time, increasing risk and cost to the enterprise. Poorly monitored collaboration tools can be an open gateway for non-compliance.



In 2016, the CFPB fined companies a total of

\$5 Billion

in penalties for non-compliance.¹³

A strong connection exists between breaches and low compliance.¹⁴



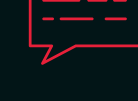
INTELLECTUAL PROPERTY (IP) LEAKS

It's Not a Matter of *If* a Leak Will Happen, but *When*.

If not secured, an ESN can open the door to leaked information, such as the following:



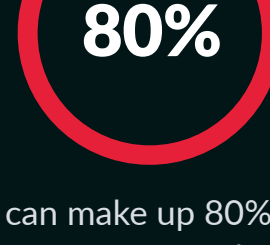
A FILE containing sensitive information accidentally posted to an external collaboration group



A CHAT regarding future business inadvertently shared with an external vendor



AN IMAGE of a product concept posted to a collaboration group with partners that are not under NDA



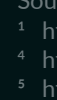
IP can make up 80% of a company's value.¹⁵



Apple recently said that more leaks come from its own headquarters than its overseas factories.¹⁶

Learn How to Protect Your Organization Against These Top 5 Enterprise Collaboration Security Risks

Download our Business Brief, *Top 5 Enterprise Collaboration Security Risks Revealed — and How to Avoid Them*, so you can have the peace of mind that your organization is deploying your collaboration and messaging tools safely — and realize the full benefits they provide.

 wiretap.com/5-risks



Top 5 Enterprise Collaboration Security Risks Revealed — and How to Avoid Them

Sources

- ¹ <https://www.margolis.co.uk/enterprise-social-networks-study>
- ² <https://www.eeoc.gov/eeoc/newsroom/release/1-18-17a.cfm>
- ³ Ibid
- ⁴ <https://www.statista.com/statistics/644351/sexual-harassment-victims-in-the-us-workplaces-by-gender-july-2016/>
- ⁵ <https://www.statista.com/chart/9469/public-perception-of-uber/>
- ⁶ <https://www.infosecurity-magazine.com/news/data-breaches-increase-40-in-2016/>
- ⁷ <http://www.nationalcybersecurityinstitute.org/general-public-interests/how-does-a-data-breach-affect-your-business-reputation/>
- ⁸ <https://securityintelligence.com/media/2016-cost-data-breach-study/>
- ⁹ <https://hbr.org/2014/09/the-danger-from-within>
- ¹⁰ Ibid
- ¹¹ <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEJ03279USEN>
- ¹² <https://www.censornet.com/solutions/shadow-it/>
- ¹³ <https://www.insidearm.com/news/00041798-total-cfpb-penalties-top-5b/>
- ¹⁴ <https://www.prnewswire.com/news-releases/80-percent-of-businesses-fail-interim-pci-compliance-assessment-300049430.html>
- ¹⁵ <https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html>
- ¹⁶ <http://www.businessinsider.com/apple-david-rice-leaks-global-security-2017-6>