wiretap

A WIRETAP BUSINESS BRIEF

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

The unprecedented collaboration afforded by Enterprise Social Networks comes with inherent risk. This paper explores the Top 5 Risks of ESNs and provides insights on how to avoid them.

**By Greg Moran,** COO, Wiretap

# The rise of Enterprise Social Networks (ESNs) and enterprise collaboration and messaging tools has brought about unprecedented collaboration opportunities to organizations that embrace them.

ESNs help break down existing silos of information, people and processes that slow innovation and kill productivity across the enterprise. In fact, McKinsey Global Institute found that companies actively using an ESN achieved impressive gains in speed of innovation, productivity, employee retention, and revenue growth — as well as reduced time spent in meetings.[1]

However, ESNs come with risk. When an organization makes internal content and ideas readily accessible to employees and business partners on an ESN, security gaps emerge. If the social network and collaboration tools are not properly secured and automatically monitored, risk to the organization is high and fallout can be costly.

Being familiar with the top 5 ESN security risks and knowing how to avoid them is the single best way for organizations to increase their likelihood of ESN success.

**COMPANIES USING ESN GAINED:**

- **31%** Faster Time-to-Innovation
- **25%** Fewer Meetings
- **20%** Higher Employee Retention
- **15%** Increased Productivity
- **10%** Revenue Growth

Source: McKinsey Study, margolis.co.uk, 2016

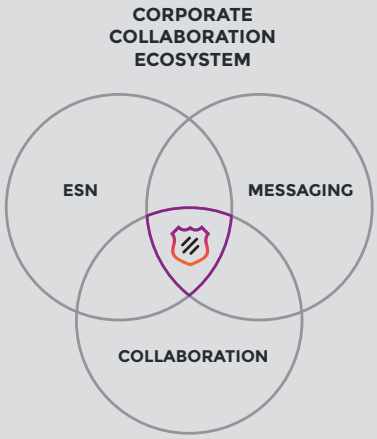
## What's included in an enterprise collaboration ecosystem?

Not surprisingly, enterprise collaboration is an emerging field of technology that's constantly changing with different terminology depending on who you talk to. The term ESN stands for Enterprise Social Network, and is also sometimes referred to as a collaboration network or a business social network.

An ESN creates a virtual community where an organization's employees and stakeholders can exchange information and ideas to improve collaboration.

Other tools in this space are sometimes referred to as messaging or collaboration tools.

Examples of tools that may make up a company's collaboration ecosystem include Microsoft® Yammer, Workplace by Facebook®, Microsoft® Teams, Microsoft® Groups, Slack, Salesforce Chatter, Jive, Skype and many others.



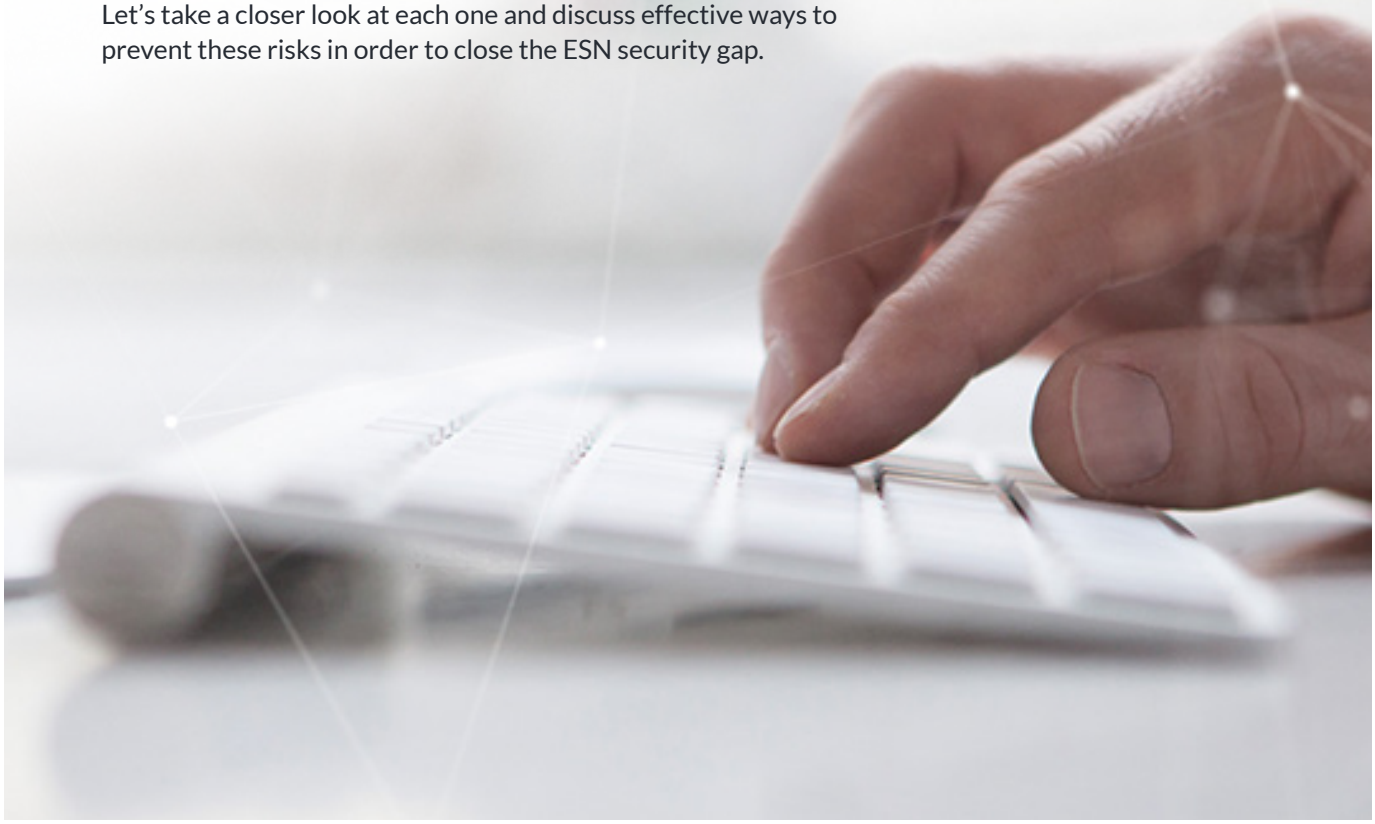

[1] https://www.margolis.co.uk/enterprise-social-networks-study

# Top 5 ESN Security Risks:
# How to Avoid Them and Close the Security Gap

Five of the most common and potentially harmful security risks associated with ESNs and social collaboration tools are:

1. HR Policy Violations
2. Data Leaks
3. Insider Threats
4. Regulatory Compliance
5. IP Leaks

Let's take a closer look at each one and discuss effective ways to prevent these risks in order to close the ESN security gap.



RISK 1

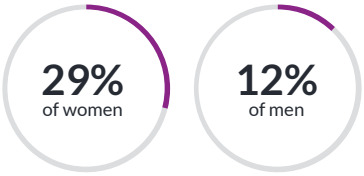
# HR Policy Violations

HR policy violations are inevitable at large organizations. Often, cases involving sexual harassment, offensive language and lewd behavior can fester for months or years before HR or top management becomes aware of it. Many harassment cases go unreported and the violated employee simply leaves. Meanwhile, the bad behavior of the offender continues unchecked — increasing risk to the organization and its people.

Consider the 2017 incident at Uber in which news of a female employee being sexually harassed by a male manager using the company's chat was brought to light. After being told repeatedly to basically "accept it," the female employee published a blog post describing systemic sexism and sexual harassment at Uber. The viral post prompted upper management to hire a former U.S. Attorney General to run an independent investigation.

The investigation not only confirmed the woman's story, it uncovered that sexual harassment was a longtime, widespread problem entrenched in Uber's corporate culture. Within minutes of the story breaking worldwide, Uber's reputation was damaged and the organization was devalued.[2] One poll found that the percentage of consumers with a negative perception of Uber jumped from 9% to 27%.[3] Other experts estimate that this and other Uber scandals have cost the company billions in lost sales and market capitalization. [4]

**IN A 2016 POLL:**




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

Source: statistica.com, 2016

> *The Anita Borg Institute, which is dedicated to getting more women into tech roles, recently cut ties with Uber due to its treatment of women employees.*

---

**This PR Nightmare Could Have Been Avoided**

If Uber had effective security controls on its internal social network and collaboration tools (the company had used Slack as well as Hipchat), this particular incident may have played out differently. With automatic monitoring and predictive analysis, either the offensive language in the perpetrator's chat messages or the impact on the victim would have been detected and flagged instantly for follow-up. With visibility into the entire data story, HR would have had all the information it needed to respond quickly and decisively — long before the situation worsened. Obviously, any company in this situation must be willing to reinforce a culture of healthy behavior in order for this to happen; however, the information would have been readily available to support the necessary follow-up.

The same premise holds true with other HR policy violations and issues — including discrimination, bullying and employee disengagement. The best security platforms allow organizations to specify granular policies against which information traveling through ESNs are monitored. This eliminates the inefficient time lags that typically exist between a policy violation occurring, it being noticed and responded to, and eventually getting resolved. As a result, the organization and its people are better protected and safe collaboration is supported.

**IN 2016:**

**91,503** workplace discrimination charges were filed in the U.S.

**$482 Million** was secured for victims of discrimination.

Source: eeoc.gov, 2017

[2] https://www.theguardian.com/technology/2017/feb/20/uber-urgent-investigation-sexual-harassment-claims-susan-fowler
[3] https://www.statista.com/chart/9469/public-perception-of-uber/
[4] http://www.cnbc.com/2017/04/25/uber-stock-price-drops-amid-sexism-investigation-greyballing-and-apple-run-in--the-information.html

RISK 2

# Data Leaks

Most ESNs come with some level of security that provides certain types of protection to the organization. Many companies don't realize that the security embedded in their ESN may not be enough to properly protect them from accidental or intentional data leaks.

The Department of Veterans' Affairs found this out the hard way in 2015 when the Office of Inspector General (OIG) began investigating the agency's unapproved use of Yammer. As it turned out, a VA employee initially deployed Yammer in 2008 without approval, and over time other collaboration networks and tools were added. Because none were secured or monitored, the ESN security gap grew.

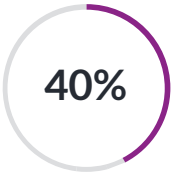
Among other things, the investigation uncovered that employees inappropriately used the ESN to share personally identifiable information (PII), including veterans' personal health information. In one incident, a user shared the VA's IP addresses. In addition, many active accounts were found to belong to former employees.[5]

**$4 Million: The average cost of a single data breach in 2016.**

Source: Ponemon Institute Study, securityintelligence.com, 2016

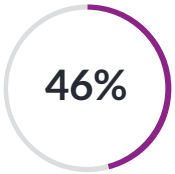
The specific number of data leaks tied to the VA's unsecured social networking over the years is unknown. It's likely that some were intentional and others were simply the result of carelessness or lack of knowledge on the part of untrained users. Either way, one thing became abundantly clear — it is a mistake to assume that an ESN or other collaboration tools are secure in and of themselves.

When the OIG's findings made national headlines, the reputation the VA became tarnished, and the VA's CIO was fired.[6]




2016 was a record year for data breaches for U.S. companies and government agencies — up 40% from 2015.

Source: Bloomberg Technologyh




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

Source: nationalcybersecurity institute.com, 2016

### Prevent Leaks by Securing Your ESN

Many of the VA's woes could have been avoided had it used a single, highly secure platform to monitor its ESNs and collaboration tools. By setting policies once, a single security platform can oversee multiple business social networks and tools, and hold them to the same security standards.

With automatic 24/7 monitoring of information shared both internally and externally, security gaps can be eliminated and rogue usage thwarted. In addition, predictive analysis built into some ESN security platforms can provide visibility into potential issues before they grow into costly problems.

[5] https://www.scmagazine.com/unofficial-va-yammer-social-network-had-security-problems/article/532804/
[6] https://www.theregister.co.uk/2015/08/24/yammer_security_substandard_says_us_vet_affairs_office/

RISK 3

# Insider Threats

Enterprise organizations have always faced insider threats from employees and business partners with ill intent or simply acting carelessly. But 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 that can be used against the company.

The magnitude of this problem is somewhat alarming. According to Harvard Business Review (HBR), at least 80 million insider attacks occur annually in the U.S. alone, costing tens of billions of dollars a year.[7] HBR further notes that the actual figures are probably much higher due to the amount of security breaches from the inside that go unreported.

The U.S. isn't alone in its growing insider threats. One recent UK study found that 58% of all data security threats came from within the extended enterprise (i.e. employees, business partners and former employees).[8]

**THE GROWING THREAT FROM WITHIN – INSIDER THREATS REPRESENT:**

**80 Million** Annual Insider Attacks

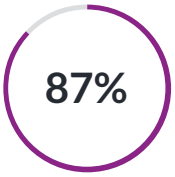
**Tens of Billions** in Total Cost

**58%** of Total Cyber Threats

## Stop Insider Threats Before They Occur

In order to succeed with an ESN, organizations must safeguard against insiders exploiting or carelessly misusing their access to sensitive enterprise information. When an ESN is unsecured, a malicious employee can simply post what they want to a private group and easily move valuable information outside the enterprise without notice. Without the proper security controls in place, employees planning a company exit might find it easy to leverage the organization's social network to garner data, customers, partners and staffing — all on the company's dime.

**IN A RECENT POLL:**




87% of respondents said they were unlikely to do business with a company that had been breached.

Source: Semafone Study, national cybersecurityinstitute.org

The best way to prevent malevolent insider attacks and careless activities is to plug the security gaps and tighten controls on your ESN. In order to do this, companies need a highly customizable security platform that oversees all business social networks and collaboration tools within the extended enterprise.

The security platform selected should continuously monitor all social content and activity it oversees and send targeted notices so that the appropriate personnel can take action. It should also have analytic capabilities to spot patterns of behavior, enabling it to predict likely future activity and prevent potentially damaging incidents before they occur.

[7] https://hbr.org/2014/09/the-danger-from-within
[8] http://www.isdecisions.com/blog/it-security/prevent-insider-threats-from-both-malicious-and-careless-activity/

RISK 4

# Regulatory Compliance

The explosive growth of data — compounded by the big data boom — has increased the regulatory burden on nearly every large organization today. From banking and financial services, to insurance and healthcare, to legal and global consulting, no industry has gone untouched. What they all have in common is that their compliance challenges are growing and changing all the time, increasing risk and cost to the enterprise.

While the cost of compliance is high, the cost of non-compliance can be much higher. Fines and penalties for non-compliance can reach tens of thousands of dollars a day in some industries. In 2016 alone, the Consumer Financial Protection Bureau (CFPB) ordered over $5 billion in total penalties, a number that continues to grow each year.[9] Furthermore, history has shown a link between non-compliance and data leaks, further raising the level of risk to the organization. [10]

Knowing this, an overburdened compliance team may be skeptical of an ESN since it can mean additional data and activities to be monitored. This can keep some companies from deploying an ESN, causing them to miss out on valuable benefits. Others might restrict features so much that the ESN becomes unusable and unable to scale to the point where it benefits the company. But there's no reason for this to happen. Companies simply need to employ a security platform that proactively monitors and supports compliance and improves audit readiness.

**$5 Billion**
Total amount in penalties the CFPB fined companies in 2016 for non-compliance.

**$185 Millon**
Total fines, and 5,300 fired in Wells Fargo fraudulent account scandal. [11]

## Increase Compliance and Improve Audit Readiness

Uncovering regulatory and compliance matters in an ESN can be like finding a needle in a haystack. But with a security platform that automatically monitors ESNs 24/7, non-compliant data and activities are brought to the surface quickly and authorized personnel are notified immediately — mitigating risk and speeding resolution.

Since state and federal regulations can change frequently, it is imperative that the security platform allows administrators select from a set of pre-defined policies as well as easily set and customize detailed, industry-specific compliance policies that enable productive collaboration. What's more, organizations should be empowered to limit certain functions for specific users that may be in highly regulated roles.

In addition, companies should pay special attention to records retention requirements. Administrators should be able to set up and control an orderly records retention and purging system — one that is customized to the organization's needs and modifiable as those needs change and grow.

Verizon research indicates a strong connection between companies that have been breached and

**lower than normal compliance.**

Source: prnewswire.com, 2015

[9] https://www.insidearm.com/news/00041798-total-cfpb-penalties-top-5b/
[10] http://www.prnewswire.com/news-releases/80-percent-of-businesses-fail-interim-pci-compliance-assessment-300049430.html
[11] https://www.usatoday.com/story/money/2016/09/08/wells-fargo-fined-185m-over-unauthorized-accounts/90003212/

RISK 5

# Intellectual Property Leaks

Intellectual property (IP) is a highly valuable asset of any large organization. It drives innovation, competitiveness and business growth — and sustains the organization over time. IP is so important, in fact, that according to Deloitte, it can constitute more than 80% of a single company's value.[12]

Examples of IP leaks abound. In 2017, Tesla brought a lawsuit against a former employee for allegedly transferring hundreds of gigabytes of confidential and proprietary information to personal hard drives and changing timestamps files in an attempt to cover up his actions.[13] Not surprisingly, the risks and costs associated with IP leaks are substantial. A single leak can cost an organization millions — even billions — of dollars, depending on the type of IP stolen and how it is used.

Two of the most common sources of IP leaks (both intentional and unintentional) are employees and business partners, the same parties that have access to internal ESNs and collaboration tools. This is another reason that securing an entire ESN ecosystem with a high-quality security platform is mission critical.


The portion of a single company's value represented by IP.

**Protect Against IP Leaks by Planning for Them**

According to Forrester Research analyst Heidi Shey, "Planning for IP theft is the best protection from it."[14] When a company secures its ESNs and collaboration tools with a comprehensive, flexible security platform, it is protecting the organization against IP loss.

Any ESN security platform should allow administrators to create specific internal and external sharing policies and set policies for immediate, targeted alerts to be sent when suspicious incidents occur. Continuous, automated monitoring of all activity and content on ESNs and collaboration tools can shut down potential IP leaks before they happen. There are many ways this type of security plays out day after day. Here are just a few examples:

- A file accidentally posted to a collaboration group that contains sensitive merger information is immediately deleted, never reaching the unintended recipients.

> Analyst Heidi Shey of Forrester Research has called the
> **theft and protection of IP "the Next Frontier for CISOs."**
> Source: searchsecurity.techtarget.com, 2017

- A chat regarding future business plans between an internal buyer and a trusted vendor is flagged for review.
- A file marked "R&D: Confidential" is blocked from being shared outside the R&D work group.
- An image of a product concept is blocked from being posted to an innovation group where images are not allowed.

When these protective actions occur, ESN users can be alerted so they become educated about internal and external compliance rules and are less likely to repeat the behavior — educating both themselves and other employees.

[12] https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html
[13] https://www.theverge.com/2017/1/26/14401612/tesla-autopilot-lawsuit-sterling-anderson-chris-urmson-aurora-innovation
[14] http://searchsecurity.techtarget.com/tip/Protect-intellectual-property-with-data-breach-prep-cost-analysis

## Conclusion

ESNs represent game-changing opportunities, including seamless collaboration across work groups and locations, faster time-to-innovation and increased productivity. At the same time, ESNs contain security gaps that bring significant risk to the organization. In order to realize the benefits and prevent the risks of business social networking, companies must employ a security platform to oversee all social networks and collaboration tools within the enterprise.

## Who is Wiretap?

**Our mission is simple: To close the security gap while making ESN adoption wildly successful.**

At Wiretap, we love collaboration — and today's social collaboration and messaging tools make it easier than ever to work together. But deploying collaboration tools within any company can open a huge security gap, so many organizations either choose not to deploy an ESN and walk away from the value of social collaboration, or patch together a system of security that was never meant to govern social networks.

Wiretap started with a basic premise — to build a solution that was meant to provide a layer of security for collaboration tools so companies can properly steward their most valuable assets — including safeguarding intellectual property and customer data, protecting employees from harassment, ensuring HR policies are adhered to, and empowering companies to follow detailed industry compliance regulations.

**We did just that, but it doesn't end there.**

Wiretap also provides a unique level of visibility into organizational sentiment so issues can be addressed immediately and positive collaboration can be encouraged — so companies can gain exponential value from their collaboration tools without worry.

*Protecting the enterprise. Encouraging positive collaboration. Providing unmatched visibility. That's Wiretap.*

### Request a Free Demo

Experience the remarkable security of Wiretap. Visit **wiretap.com**, email **hello@wiretap.com** or call **844.433.3326** to request a demo.

**wiretap.com**