The People Factor—Menace or Protector?

People. Process. Technology. It's been the mantra of businesses for decades. The challenge is to have a balance of all three—technology is only as good as the processes, which are only as good as the people.

Today it starts with the right people committed to corporate governance processes that facilitate collaboration and ensure content protection for emails and documents at rest…in transit…and in use through a technology-enabled cloud solution.

People. Process. Technology. People. Game changer. Now we have a 50% increase in The People Factor—and people-based risk. It's become a lot more complex.

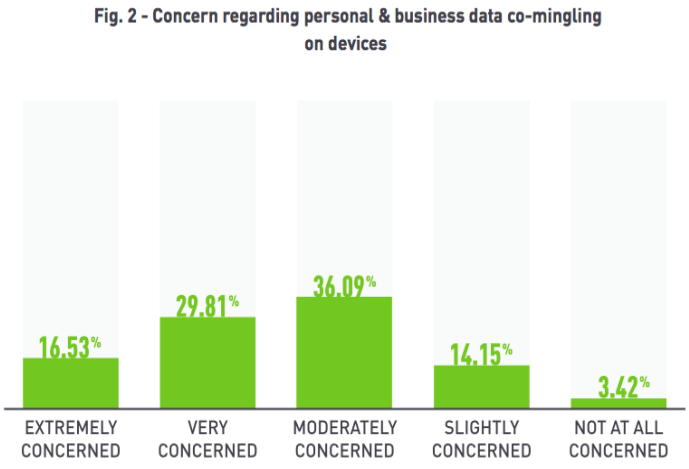
Now it's all about digital technology and cybersecurity. More people. More endpoints. More chances for information to get into the wrong hands. We need protection against attacks.

It's about the need for people to be engaged at the front end to set strong security policies and implement the right technology solution to protect content. To meet national and international compliance regulations like NIST SP 800-171 and GDPR, it's critical to combat cyber threats with a content protection solution—implementing processes that ensure intellectual capital and personally identifiable information are persistently protected.

It's about the need for people to implement watchdog procedures to mitigate risks on the back end, safeguarding private information inside and outside the firewall.

It's about the ever-increasing Bring Your Own Device (BYOD) trend where everyone wants to stay connected all the time and as a result connects their devices through enterprise networks. Creating innocent data leakage—through the technology infrastructure. These new digital demands up the game every day for IT departments.

Concern regarding personal & business data co-mingling on devic



Source: *The 2017 State of Cybersecurity*, Forcepoint

And it's about the interaction between data and human behavior. What?

Yes. The newest analytical research tool on the block is understanding The People Factor—how people interact with data. Sometimes a breach is accidental. And sometimes it's done with malicious intent. Either way, the invasion is serious business. The Forcepoint *2017 State of Cybersecurity* whitepaper reveals that "learning how users interact with critical data is a rising priority…and the understanding of this behavior and intent is vital to cybersecurity."

We've reached a crossroads between information technology and behavioral science. Who'd of thunk it!

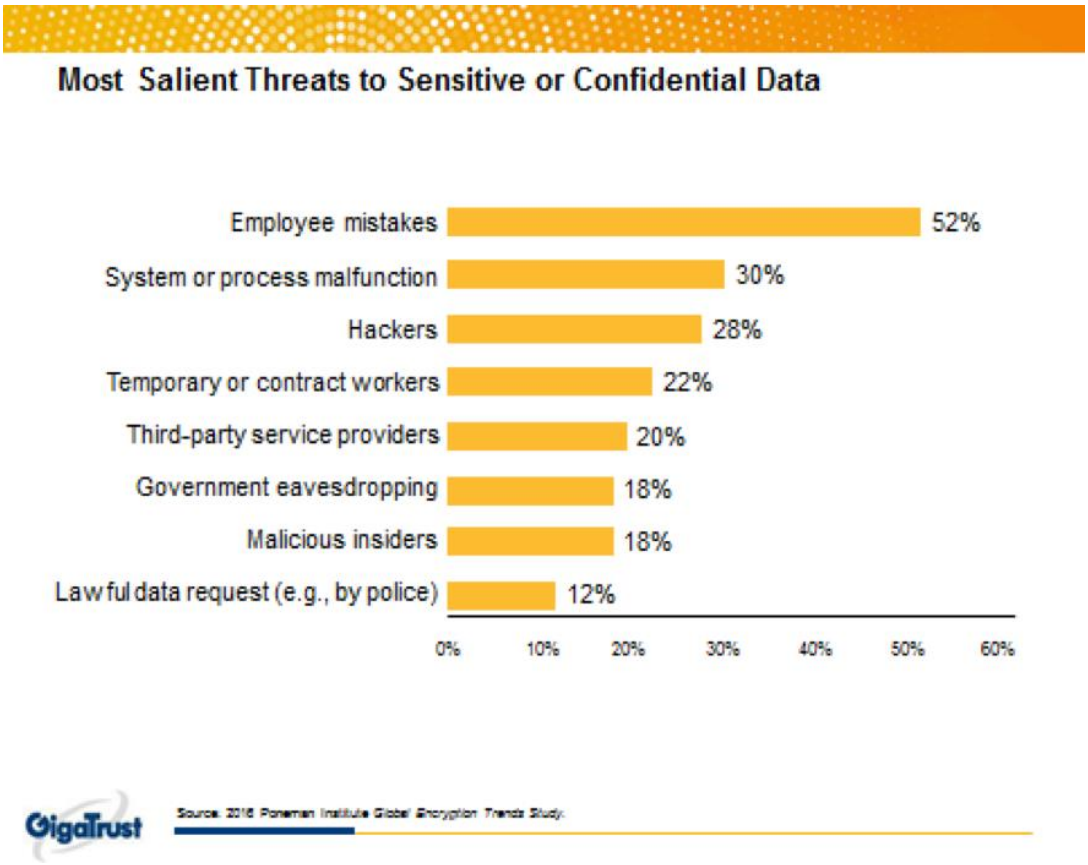
It's in black and white in *Nature*. The international weekly journal presents the case that if we implement the right processes and technology, but we are still facing threats, then we need to focus on human errors, like weak passwords or spear phishing. The Department of Homeland Security (DHS) is even in the mix. According to division director Douglas Maughan, "too many computer scientists are looking at cybersecurity and not enough psychologists, economists and human-factors people." Funding for research into the human side of cybersecurity has increased over the past five years at DHS. And the Research Institute in Science of Cybersecurity (RISCS) has a £3.8 million (U.S. $5.5 million) grant from the UK government to study cybersecurity in businesses. The People Factor is global.

Why The People Factor outweighs process and technology

According to Gartner estimates, worldwide spending on information security is expected to reach $90 billion in 2017, an increase of 7.6% over 2016—and top $113 billion by 2020. Bloomberg reports that more security spending should theoretically result in fewer incidents, yet U.S. companies and government agencies suffered a record 1,093 data breaches in 2016—an overwhelming increase of 40% from 2015. Despite new cybersecurity investments in process and technology, cybercrime continues to increase—overwhelming proof that the quest for new and ideal security technology is still a challenge. Pointing to The People Factor—the constant in the equation.

Where does the menace come from?

The People Factor. The menace is people. External data breaches and hacking are a constant threat from competitors, state-sponsored hacking groups and criminal hackers. It could even come from contractors sharing proprietary information. But employee mistakes are the number one reason for data breaches. That's why a cybersecurity awareness program is mission-critical to combat bad behavior.



The Forcepoint Cybersecurity whitepaper data shows that "…one-third of enterprises have suffered from an insider-caused breach, with possible losses from each incident amounting to more than $5 million, according to the SANS Institute." Forcepoint divides insider threats into three groups. Makes sense.

1. **Accidental Insiders –** people who make unintentional mistakes due to lack of training, awareness and familiarity with processes or negligent behavior: **inadvertent actors** who make honest mistakes or **convenience seekers** who put data where it shouldn't be.
2. **Compromised Insiders –** people with access to the network whose credentials have been stolen and used by an attacker to penetrate or misuse the system: **malware victims** targeted or infected with phishing emails or **impersonated users** who had credentials stolen.
3. **Malicious Insiders –** people who have knowledge and access to organizational resources and are discontented: **rogue employees** who carry a grudge or **criminal employees** who conduct corporate espionage.

Where does cyber protection come from?

The People Factor. The protector is people. This infographic from Kaspersky does a good job of capturing the greatest fears of businesses these days and ways to stay protected.

Best-case scenario: Trustworthy employees who are well-informed about company security processes and behave in a conscientious manner to ensure content protection. That's good behavior. An effective cybersecurity program includes top-down leadership, endpoint security technology and employee process training.

So, what's The People Factor? It's made up of all people. Some bad. Some good. The People Factor includes those who create the menace—and those who provide the protection. A conundrum. We need to join forces to ensure good behavior gets rewarded.

The GigaTrust™ flagship service, GigaCloud™ delivers persistently protected emails and documents for collaboration anytime, anywhere, to anyone on virtually any device and serves as the foundation of a well-rounded cybersecurity culture. We're part of The People Factor that makes the world a safer place.