IT Security

Data security is often a top concern for management. Security breaches can end up threatening the livelihood of employees and entire companies alike.

Mobile security

As mobile usage grows, and internet availability increases, organizations are expected to increase awarness and have the right tools and policies in place

Mobile has become an essential aspect of almost every business, and an astonishing 132 million people around the world use their smartphones at work

Limiting mobile access, and regulating VPN access is a necessity to fight against outside threats

Numbers Don't Lie

75% of office workers upload work files to a personal email or cloud service

75%

Of organizations view employee negligence as the greatest breach

Human error continues to be the biggest source of data breaches

Common outcomes of a security breach

- Lost operational time
- Loss of business focus
- Loss of customer confidence
- Loss of business opportunities
- Damage to employee morale and confidence
- Time spent in activities to recover
- Technical and Legal fees for dealing with damages
- The cost and time involved in recovering back to normal

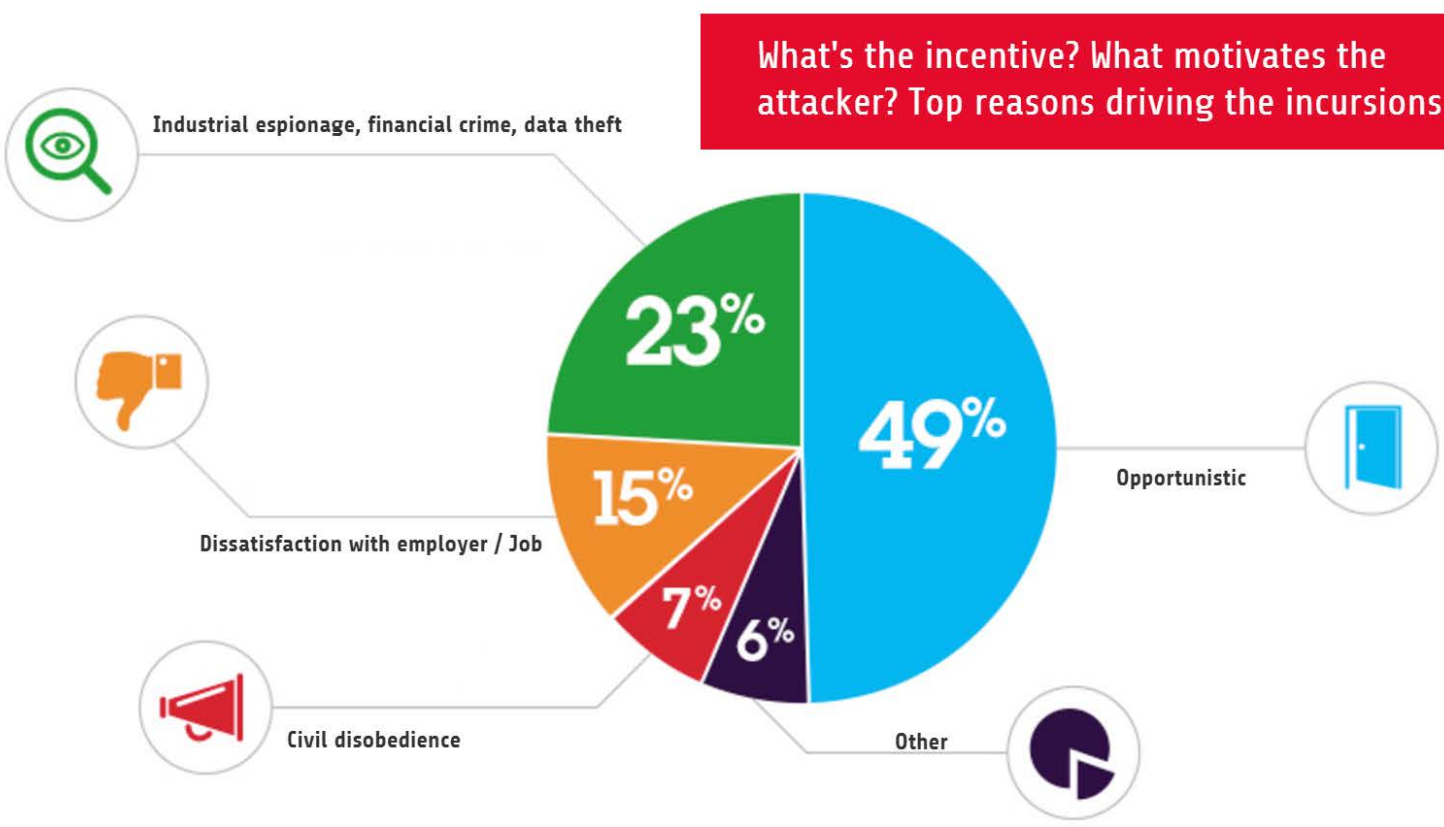
Malicious insider attacks can take more than 45 days to contain.
One of the worst things a company can lose to a hacker, is its hard earned reputation.
Rebuilding BMMI's brand can cost thousands in:
*Public relations expenses
*Customer and shareholders outreach efforts
*Defending the company in liability suits

As much as 80% of important corporate data should reside on company protected services such as SharePoint & OneDrive (which is to be launched before the end of the year) to be properly backed up and protected.

5 Most Attacked Industries

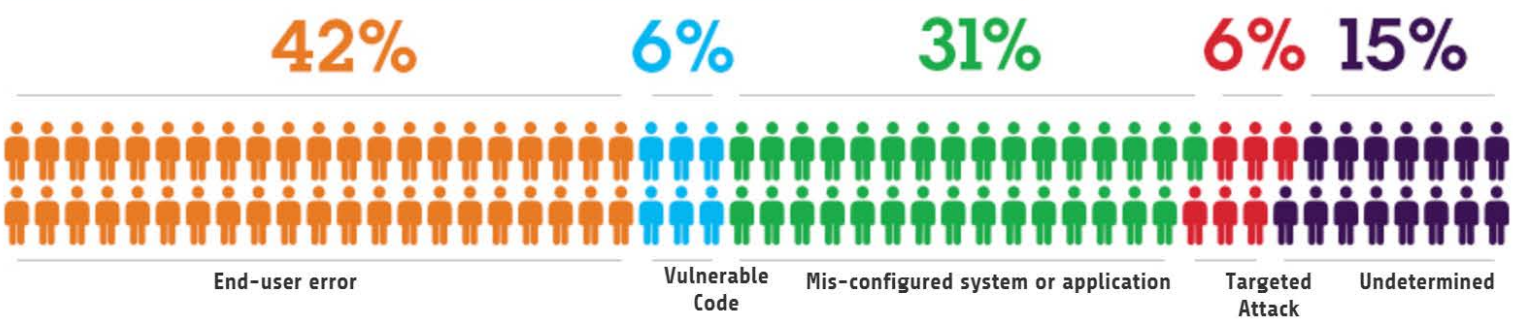
Manufacturing	Finance & Insurance	Information & Technology	Health	Retail & Wholesale
26.5%	20.9%	18.7%	7.3%	6.6%

What's the incentive? What motivates the attacker? Top reasons driving the incursions.

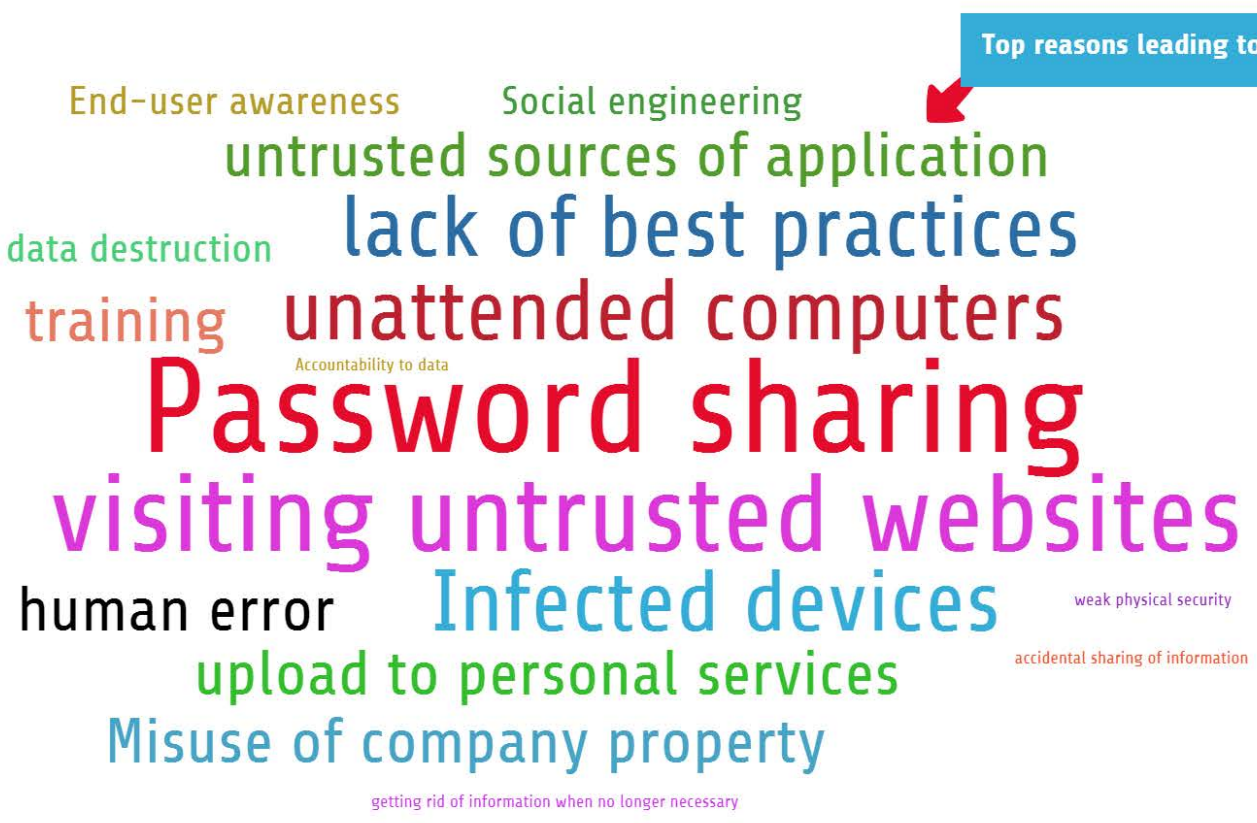


How do breaches occur?

Many elements can contribute to the vulnerability of our organization, however none is more prevalent than the human factor, which accounts for approximately **80%**



Top reasons leading to attacks



What can you do to reduce the numbers in your favour?

Build a risk-aware culture, at company level.

There should simply be zero tolerance at a company level when colleagues are careless about security. Management needs to push this change relentlessly from the very top down.

Manage incidents & respond

Launch a company-wide effort to implement intelligent analytical capabilities, through a unified system, governed by policies & procedures to respond accordingly to internal and external threats.

Avoid common mistake:

Treat the company property as if it was yours. Any harm to this property will impact you, your colleagues and the company as a whole.

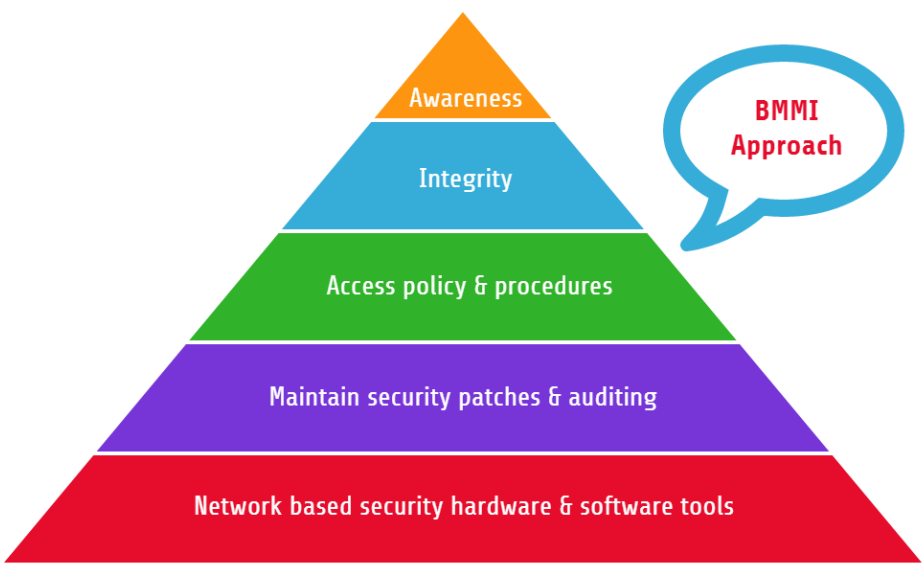
IT policies & procedures are being further developed to protect your best interest and the Group.

Let best practice be part of your normal day to day work.
Changing your passwords when requested protects your account from random access by others, and NEVER share your passwords!
When you receive a suspicious message or email, report it immediately.
If you notice a suspicious behaviour, report and be as descriptive as possible, to enable Helpdesk and IT to provide the necessary steps.

Avoid installing random applications on your laptop and personal mobile device. Always make sure that your anti-virus is updated.

Immediately report if

- Some known pages are redirected to other strange pages.
- You cannot login using existing credentials, even when you're 100% sure from the login details.
- Strange keywords/files/icons appear without warning.
- When colleagues inform you about sent messages, and you know you haven't sent any.
- When you notice the anti-virus application disabled.



Its crucial to acknowledge that data security in the workplace is not just the IT department's responsibility or reputation that is under threat. As head of IT, I can put the protocols in place to secure our data and ensure that we are following the best practices, and have the right tools to keep us safe from external threats. But a bigger responsibility requires the awareness and understanding of our people to ensure that our intellectual data and workplace is secure from external threats, and not at risk internally due to misuse of BMMI's technology properties.