imagine IT

The Q2 2025 State of Cybersecurity

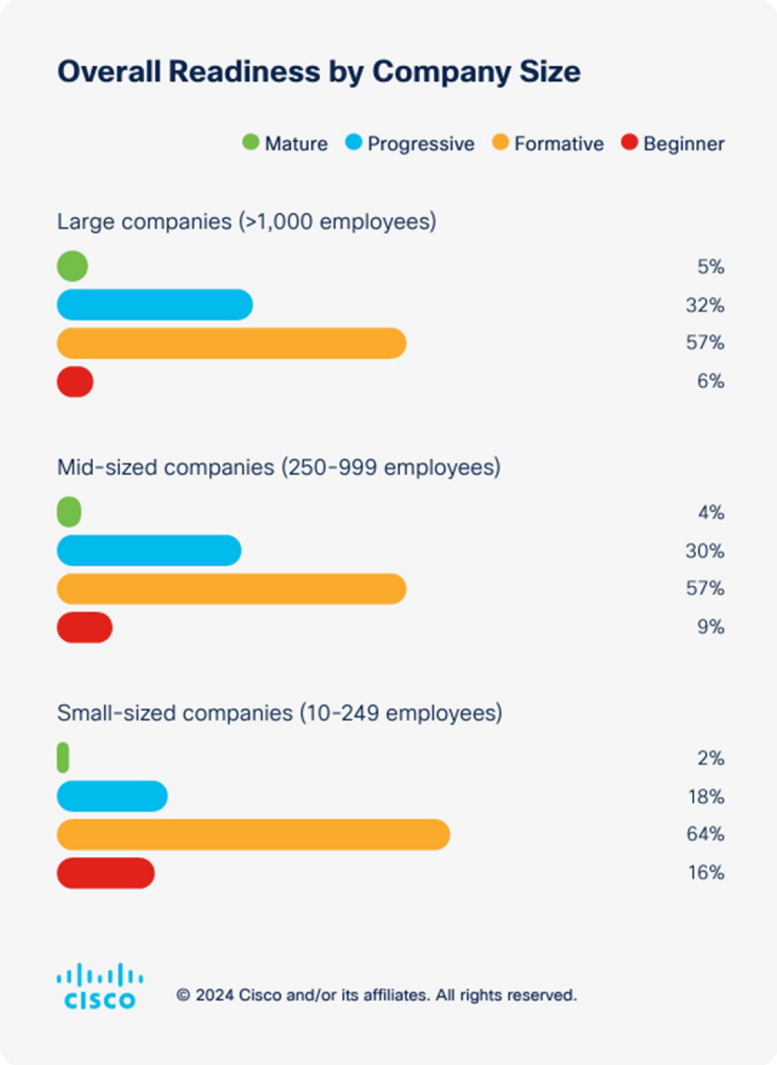
imit.com

Cyber-Criminals Are an Iceberg – Is Your Org the SS Minnow?

Per Cisco in 2024, only 2% of small US orgs can defend and respond to modern threats. That means the remaining 98% are low hanging fruit to cyber-criminals.

Which side of that fence is your org on? I think we all know.

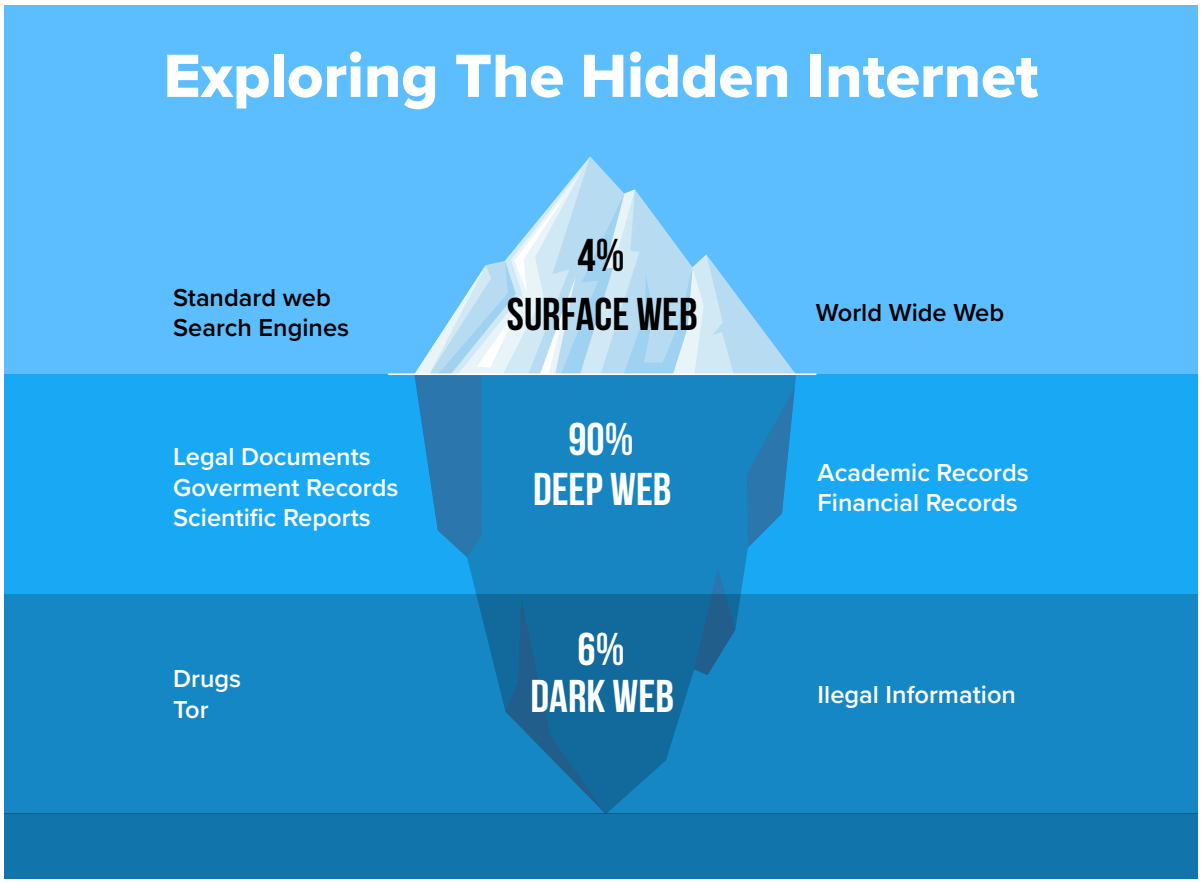
How is it that only 2% can defend? This is due to their massive cybersecurity budgets, large teams, and mature processes (we are talking multi-million-dollar annual spend and teams of hundreds).



And even the 2% experience large-scale cyber incidents. How is it that cyber-criminals have become so powerful they can succeed against the 2%?

It's the Dark Web.

What is the Dark Web and Why Does it Increase Cyber-Criminal Power?



Notice the Dark Web (6%) is actually larger than what search engines can access (4%). Insane.

Cyber-criminals use the Dark Web to:

- Conduct illegal activities
- Sell access & stolen credentials
- Sell confidential & sensitive data
- Sell hacker tradecraft
- Setup affiliates with a commission structure

Until recently, only a handful of elite hacker groups had the acumen for complex attacks. But now those veteran hacker groups have shared their tradecraft with the less mature groups, and even setup franchise systems. Now there are over 100,000 skilled hackers, all following the proven blueprints.

Cybercrime has become so massive that it is now considered the third-largest economy globally, after the US and China.

How to Avoid Being Low Hanging Fruit

Does your org have a multi-million dollar cybersecurity budget to obtain top 2% status?

Of course not. So how do you successfully defend?

Answer: Budget to upgrade your org's cybersecurity posture into the top 10% (this has a reasonable cost), which elevates you out of the low hanging fruit.

Here is a high-level plan...

- Make a truly serious effort to protect your systems and data. This is a strategy that must come from the C-suite.
- Meet 90% of Cyber Insurance requirements. In particular...
  - MFA (Multi-Factor Authentication) everywhere.
  - 24/7 Detection & Fast Neutralization (<15 minutes) on computers and in M365 & Google Workspace.
  - SIEM (Security Information & Event Management).
  - DNS Security/Filtering.
  - Advanced Email Security scanning & banners (not just SPAM filtering).
  - Automated Security Awareness Training & Phishing Exercises.
  - Recurring Vulnerability Scanning or Penetration Testing.
  - Dual-authorization for banking changes, and a process to ALWAYS CALL (via a phone number already documented) anyone requesting to change banking information.
- Bottom Line, make your org an unattractive target by frustrating criminals during an attack.

For example, if an attacker gets into one of your user's computers but cannot laterally spread or elevate privileges, they will likely give up.

The organized hacking groups run it like a business, and they will move on to an easier victim where they can make money faster.

Conclusion

We all know the story of the unsinkable Titanic. If cyber-criminals are an iceberg, every org is at risk. However, since organized hackers want fast, easy wins, they target orgs with perceived weak security – the low hanging fruit – the SS Minnow. Don't be Gilligan.