Visibility, Intelligence, Control

Three steps to measuring digital risk against digital opportunity
Risk = Likelihood x Impact
Understanding risk is simple. Identifying it – not so much. But risk is your responsibility right? So as long as they’ve got you, other departments don’t have to worry about risk… right? They can focus on finding the new digital initiatives that will keep your business moving.

That’s great for them. For you, it can be another story. It’s up to you to make sure your business can pursue these new opportunities with confidence. So, when you look at today’s leading digital initiatives, you probably see things a little differently… Knowing the risks is just the start. Next is applying the equation to weigh the risks up against the opportunity – and no two initiatives are ever the same.

Wondering where to start? Read on to find the steps for measuring digital risk against digital opportunity.
Visibility, Intelligence, Control
Three steps to measuring digital risk against digital opportunity

1. Visibility
What solutions have you deployed that help you identify the risks of a digital initiative?
This is usually a mix of technologies and static processes. Start by taking stock of them all (and their insights). Then, you’ll have a better understanding of how well you can spot and handle emerging risks in areas like:

- Real time visibility of users, devices and usage
- Cloud adoption
- Apps and infrastructure endpoints
- Encrypted traffic
- Movement of company data

2. Intelligence
How will you analyse the issues and what do you need to measure risk against opportunity?
If you work in security, it might be as simple as getting your hands on a vulnerability scanner. A quick once over will likely reveal a load of potential issues. Of course, you’ll have to consider each one carefully – some will apply to your new digital initiative more than others.

To figure out which should make it on to your list, keep the risk equation in mind. What are the odds of the risk becoming real – and what would that mean for your business?

3. Control
What are you going to do to treat the risk?
Once you’ve got your list, you can prioritise the risks – riskiest to least risky. If you’ve gathered all your insights and applied the risk equation to each, this should be the easy bit. For each, pick one of the following options:

- **Mitigate.** Put a safeguard in place to reduce the likelihood or impact of the risk.
- **Accept.** Maybe the likelihood or the impact of this risk is negligible. In which case, a disaster recovery process might be the better option.
- **Transfer.** Outsource to a third party and let them manage the initiative (and the risk) for you.
- **Avoid.** If the risk is too likely or too great and there are no safeguards up to the task, well, maybe this digital initiative isn’t for you.
The bigger the opportunity, the greater the risks. And sometimes, you don’t want to go it alone. Whether it’s to close a skills gap or just to get a second opinion, more and more businesses are turning to a security partner to build their risk-based approach to digital initiatives. To lend a hand, BlueFort Evolve offers enhanced support to augment your cybersecurity teams and technology.

With an IT skills gap only getting wider, many organisations are enjoying the flexibility and security of a service that’s more enhanced than break-fix support but not as expensive or in depth as a traditional managed service. BlueFort Evolve provides a greatly enhanced, tiered level of service, offering you help and advice when you need it the most, in a flexible consumption model tailored to all.

Our Evolve service is uniquely customisable; each level comprises of a number of entitlements and inclusive Evolve Credits that you can use as and when you require them.

The flexibility provided by BlueFort Evolve allows you to only outsource what you need so that your technologies can be configured and supported to their optimum. By transforming your organisation’s security posture with direct access to technical expertise you can see a true return on your investment.
As a full service IT Security Integrator, BlueFort are able to deliver end to end security solutions to meet your cyber security objectives. Our focus on carefully selected technology partnerships enables us to be considered subject matter experts of those technologies, and therefore we are uniquely positioned with the insight and expertise to craft innovative solutions to secure our customer data as fully as possible.

A sample of these technology partners can be found below:
At BlueFort, we can support you through the three steps of gaining full visibility, applying intelligence, maintaining control – and beyond. Identifying risks, assessing their impact, and deciding on the right course of action.

Once you are on your journey we have a range of services that are more enhanced than standard break-fix support and more affordable and flexible than a traditional managed service to ensure you are optimising your security investments.

Our technical experts can support you in a variety of capacities, offering a comprehensive portfolio of services including installation, configuration, testing, implementation, training and ongoing support.

To find out more about how we can help you balance the risk against the opportunity, get in touch with one of our consultants:

- enquiries@bluefort.com
- 01252 917000
- bluefort.com
Find out more:

✉ enquiries@bluefort.com
📞 01252 917000
🌐 bluefort.com
🐦 BlueFortSec
LinkedIn BlueFort Security Ltd