



THE UNITED WAY OF

TARRANT COUNTY CASE STUDY

After a cyber-attack, the United Way of Tarrant County needed a helping hand.



1 Problem

After a security incident in which fortunately no donor data was compromised, the United Way of Tarrant County realized they were vulnerable to cyber-attack and needed to strengthen their security posture.

2 Solution

Makaye Infosec created a security roadmap that identified key areas to protect and broke efforts down into palatable action steps that fit within UWTC's timing and budgetary needs.

3 Benefits

- Better security: An above average infosec rating as compared to their competitive set nationally
- Confidence: Knowing that they are successfully protecting donor information
- Cost-effectiveness: Access to enterprise-grade security at nonprofit-friendly pricing

OVERVIEW

The United Way of Tarrant County (UWTC) works tirelessly to improve the lives of people in their local community through a variety of charitable efforts. The organization coordinates individuals, groups, donors, and service providers together to address and help solve tough social issues affecting Tarrant County – including housing and homelessness; health and wellness; education; and more.

But they were vulnerable to attack in ways they didn't realize or expect. "Back then we'd say, 'Why do I need an infosec effort? I'm not selling a product, I don't have a storefront,'" says Jeff Allison, Chief Financial Officer of UWTC.

CHALLENGE

But cybercriminals don't discriminate, and UWTC's IT systems were breached. Though no donor data was compromised, they knew they might not be so lucky a second time. And they had no choice: they had to protect their donor information.

"There's zero give on that," says Allison. "It would only take one breach to lose donor data, and that's our entire business reputation."

But UWTC was less familiar with information security than with IT operations generally, and in the beginning – facing multiple potential points of vulnerability – the work felt overwhelming.



SOLUTION

Makaye Infosec carefully walked UWTC step-by-step through fortifying their security posture, starting with an initial assessment of vulnerabilities. The organization identified key areas in need of protection – including policies, Cloud, IT controls, donor information, key applications, backup planning, and more – and developed a comprehensive roadmap.

With a course charted, Makaye Infosec and UWTC began breaking the roadmap down into achievable, bite-sized actions. UWTC realized that they needed in-depth protection and that the roadmap would take time – as much as a year or more – to fully implement. “You have to have a security presence that’s more than just a firewall, antimalware, basic monitoring, more than just changing your password,” says Allison.

That meant Makaye Infosec needed to work closely with UWTC’s existing IT services provider to coordinate and collaborate when needed – supporting each other – while providing critical security oversight. By splitting the disciplines, each group could focus fully on their own specialty, while still coming together in, as Allison puts it, “a really powerful way.”

There was a lot of ground to cover. Makaye Infosec helped UWTC to develop upwards of 100 new security-related policies. It also meant helping UWTC to understand their vulnerabilities and risk factors and what security measures were necessary to take at each step in the roadmap.

Underlying all efforts was the key understanding that cybersecurity is a form of risk management and mitigation. “For me,” says Allison, “infosec is an extension of my internal control environment.”

That meant developing and deploying security protocols and practices customized to UWTC’s unique situation as a not-for-profit operating on thin margins and for whom donor trust is an existential concern. In the end, Makaye Infosec’s approach to cybersecurity was successful: “It made the infosec work really fall into place nicely,” says Allison.



RESULTS



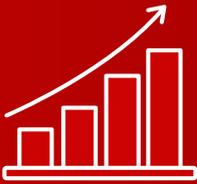
Improved Security

"In our case, we went from a very poor infosec rating to, now, a very good rating, and we have a plan to keep improving."



Cost-Effectiveness

"I can work at the pace and cost that I want. I've found everything with Makaye Infosec to be very cost-effective."



Better Rates

"We get a better quote with our [cyber] insurance coverages because they see what we're doing."



Confidence

"We have measurable metrics that we can look at to validate and ensure the protection of our donor information."

"I won't say the number, but our initial security rating exposed how vulnerable we were. We've now improved that rating to 'above average' for our competitive set nationally."

**Jeff Allison, Chief Financial Officer of the
United Way of Tarrant County**



Your Trusted

Cybersecurity Partner

If you need help addressing your cybersecurity concerns, Makaye Infosec has extensive knowledge and expertise in securing and protecting nonprofits.

Contact us today for a **free consultation** and find out how a **Cybersecurity Maturity Assessment** can help you secure your organization.



George Makaye, CISSP

smla@minfosec.com

(972) 645-2218

www.minfosec.com