

## Business of Technology Use Case: **Cybersecurity**

To help accelerate the adoption of emerging technologies, CompTIA members have created a series of use cases that highlight examples of solving real-world business problems and how you can do the same.

macnamara®

# From Traditional MSP To Technology Partner:

*One Company's Journey to Success*

In this edition, you'll learn how a traditional MSP recognized a gap in its portfolio and made necessary investments to add security expertise, transforming the company into a total technology partner.

### OVERVIEW

Macnamara ICT is a well-established managed service provider in the U.K. with more than 15 years specialising in SME clients. As technology and business models have changed, it became clear there was an important gap in the MSP's portfolio—security, especially after the development of Cyber Essentials, a U.K. government-backed information assurance initiative, that put more emphasis on security.

The company knew it had to reinvent itself, investing in training for employees not only on security technologies, but also on security policies, procedures and protocols vital to ensuring customers' protection. All this at a time when SME IT budgets in general were very limited, let alone for devoting additional resources to security.

### CHALLENGE

The need for solid cybersecurity solutions has become paramount in companies of all sizes. While many SMEs may now understand what they need and why they need it, they don't know how to manage it, according to Ciaran Kenny, managing director of Macnamara. Cyber Essentials provides an excellent baseline for businesses to follow, but it's also important to ensure that security controls are maintained.

That's where many SMEs struggle, because standard tools are often way beyond their technical and budgetary reach. As a result, security assurance can be very hard to achieve for smaller organisations.

“There’s increased awareness among clients that they need to address security but there’s not a dynamic urge to do anything about it,” said. “We wanted to take the initiative to fill that gap, but we weren’t a security company.” As Macnamara knew, you don’t just become a security specialist overnight. Compounding the challenge was the fact that customers want to do more on their own, and tech giants like Microsoft, Google and Amazon have changed the way people look at IT.

“We’re making the transition from traditional MSP to a technology partner to our customers. What we set about doing was a slightly scary conversation both us and our customers. We had to admit that we don’t have security expertise, but let’s talk frankly about how to address it,” Kenny said.

### SOLUTION

To evolve from an MSP to a technology partner with a security focus, Macnamara had to invest in its team. That meant security and industry certifications for its technical team, as well as identifying and adding security products to add to its portfolio. For the latter, the company partnered with Lujam, which helped establish a security monitoring practice for Macnamara that ranged from computer networks to non-PC process controls, greatly enhancing the MSP’s value to customers.

“We have invested in high five figures now and we see spending on training as a key budget item going forward,” Kenny said.

For one food processing customer, Macnamara separated process controls and computer networks to avoid specific security risks around the process control systems, which tend to be insecure and rarely patched. “We also identified the data flows associated with those process controls and did so without disrupting close to 24/7 operations,” Kenny said. “That’s something we had not been able to do before.”

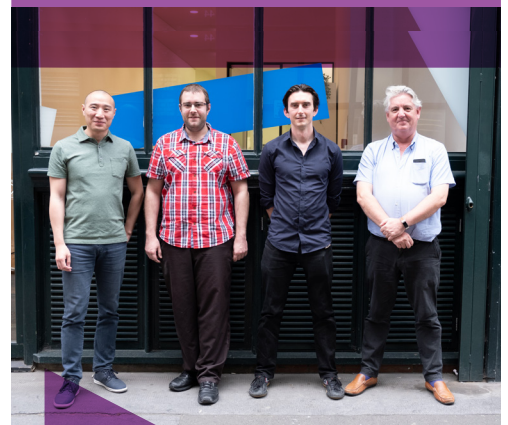
Macnamara also set about implementing new processes and policies that changed the way the company talked to customers. Instead of saying no to requests it couldn’t handle, they said OK, we can do it, but we’ll have to do this too, Kenny said.

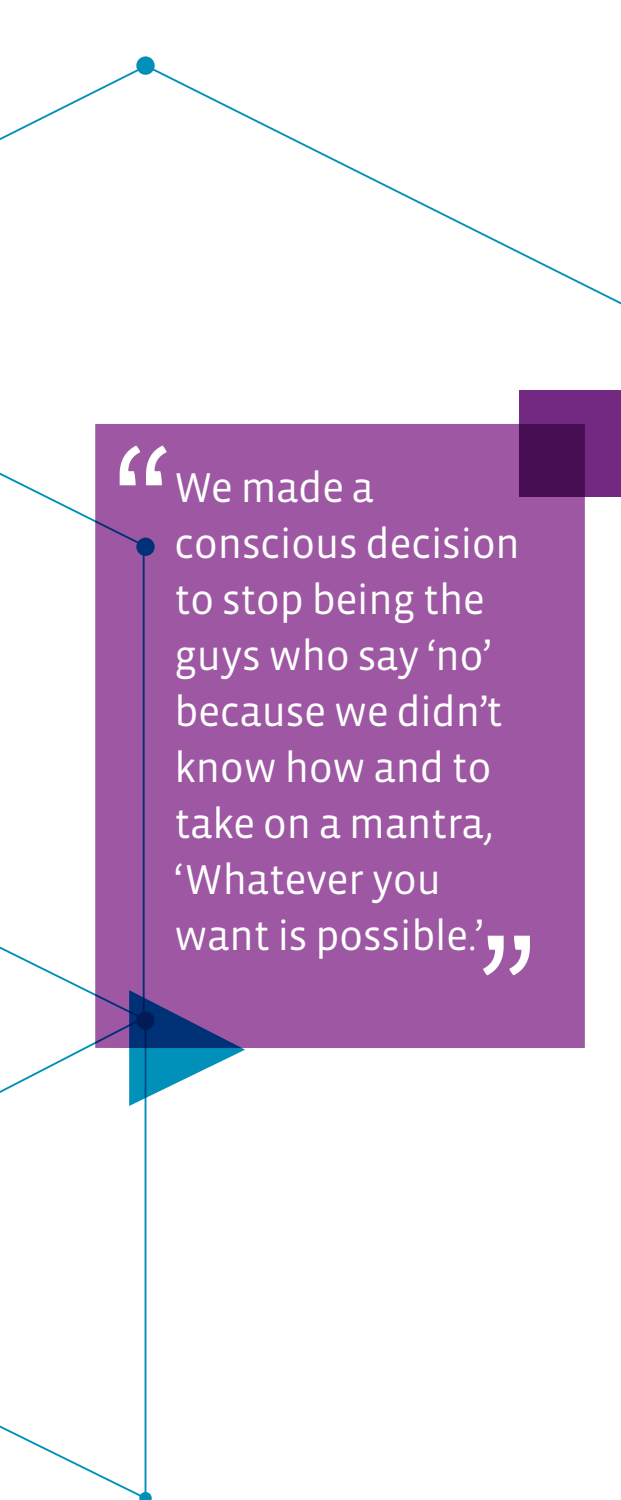
“That was a lot of retraining for our team. Not so much on technology, but on processes. It was one step at a time, with a degree of resistance at first. IT people are all about service. We were kind of changing the paradigm in the company to say we’re not all about technical service. We’re trying to be more professional service than technical service,” he said.

There’s a side benefit to focusing on customers in a different way, Kenny said. Macnamara itself became more productive and efficient. The company went through an external audit which helped identify its own security gaps to address.

“By focusing on our own information security, we are in a far healthier place in terms of control of information, which of course is the lifeblood of what we do. We spend less time on passwords and finding information and more time being proactive,” Kenny said. “As a small team, it was a transformative experience for

“We’re making the transition from traditional MSP to a technology partner to our customers. What we set about doing was a slightly scary conversation both us and our customers. We had to admit that we don’t have security expertise, but let’s talk frankly about how to address it.”





“ We made a conscious decision to stop being the guys who say ‘no’ because we didn’t know how and to take on a mantra, ‘Whatever you want is possible.’ ”

the guys. The experience of being audited and passing the audit was very good for morale and for the business.”

#### **OUTCOME**

Looking forward, Macnamara is now able to offer more robust security monitoring to more non-traditional devices and systems, a new skill that has helped to differentiate the company in its market.

“Control systems have the potential to be misused and can pose a higher risk on the network, but we are able to use LuJam in conjunction with the firewall solution to identify and, if necessary, block any traffic of concern,” Kenny said.

The investments have paid off. The company has changed its value proposition to its existing customer base and is now looking to market itself as a security expert to new prospects.

“We made a conscious decision to stop being the guys who say ‘no’ because we didn’t know how and to take on a mantra, ‘Whatever you want is possible,’” Kenny said.

The company also stepped out of its comfort zone by marketing itself as both a technical and a business expert—writing blogs on topics such as practical help for office managers. They also started a monthly webinar for customers to keep them up to date on the latest risks and how Macnamara is responding.

“It’s been successful. Now, when we tell people these are the rules around security, they don’t argue. They know we’re not being pernicky IT people; they understand we’re thinking about their security, their success,” Kenny said.

#### **SUMMARY**

Macnamara has successfully transformed itself into a trusted security advisor. By including LuJam in its service stack, Macnamara has improved its security assurance to clients and is now maintaining compliance with Cyber Essentials+ for customers.

“This is just beginning to bear fruit. We’re just at the start of this security journey. We’ve just taken on our first new sort of customer, one that we would have steered clear of in the past because they were running a lot of shadow IT,” Kenny said. “And all our existing customer base have a much better understanding that we care about them.”

#### **WHAT’S NEXT**

Macnamara plans to develop a comprehensive training initiative for customers. “We want to empower end users through workshops on security awareness, and their managers through online training that goes a bit broader and deeper into security management,” Kenny said.

For other solution providers struggling to transform their company the way Macnamara did before building a successful security practice, Kenny advises to question the fundamentals of your business. It's not easy to admit you can't do something well, but that's the first step towards true change.

"As MSPs, we're all aware that the ground is shifting beneath us quickly. We just have to accept that the Googles and Amazons have completely changed our world. We couldn't go on picking a tech stack that suited us but maybe not our customers. That's led us to where we are now," he said.

#### ADDITIONAL RESOURCES

##### **Build, Buy, Partner: Best Practices for Hiring and Retaining IT Security Staff (video)**

<https://www.comptia.org/content/build-buypartner-best-practices-for-hiring-and-retaining-it-security-staff>

##### **Data Breach Response Planning Guide**

<https://www.comptia.org/content/guides/data-breach-response-plan>

##### **Emerging Technology Innovation Assessment Quiz**

<https://surveys.comptia.org/s3/Emerging-Tech-Assessment-Grid>

##### **How Every MSP Can Implement AI to Reach Business Goals (blog)**

<https://www.comptia.org/blog/artificial-intelligence-chatbots>

##### **MSPs Are Under Attack from Cybercriminals, Here's How They're Protecting Themselves (blog)**

<https://www.comptia.org/blog/msps-are-under-attack-from-cybercriminals-here-s-how-they-re-protecting-themselves>

##### **Cybersecurity for Digital Operations (research)**

<https://www.comptia.org/content/research/cybersecurity-for-digital-operations>



Macnamara ICT invested in its future, adding cyber-security skills through retraining employees on both security technologies and business processes to better serve customers. It's a journey that other solution providers can take as well by following these steps:



Invest in your team. Make training a key budget item and educate employees on security technologies, policies, procedures and protocols.



Learn to talk to customers in a different way—strive to be a business partner, not just a technology partner.



Perform an external audit to identify your own security gaps and address them.



Teach your customers and potential customers about security awareness.



Update your value proposition and marketing efforts to reflect your new offering.