Computacenter

5 QUESTIONS YOU SHOULD BE ASKING ABOUT YOUR CYBER SECURITY

ABOUT COMPUTACENTER

Computacenter TeraMach, Inc. has over 24 years of experience in the public sector, education, healthcare, and commercial industries, focusing on Digital Transformation in the areas of Security, Cloud, and Edge. Our extensive data center technologies' experience, digital services capabilities, strong vendor relationships, and deep technical knowledge has enabled us to be the trusted partner for our 2000+ satisfied customers.

Computacenter is a leading independent technology partner, trusted by large corporate and public sector organizations. Together, we help our customers to source, transform and manage their IT infrastructure to deliver digital transformation, enabling people and their business.

TABLE OF CONTENTS

QUESTION 1:
WHAT ARE MY CYBER SECURITY GOALS?

Eli Goldratt's book, The Goal, is listed as one of the most influential business management books of all time by Time Magazine. Its lessons are applicable beyond manufacturing and among those lessons is that every decision must aim at furthering the institution's Goal. This is not as simple as it sounds. Distractions are constantly trying to take your focus away from the Goal.

But what happens if our Goal is ambiguous or not clear to stakeholders? In the absence of a tangible Goal, our focus is diverted towards other problems and eliminating these becomes the Goal. What we perceive as important are often things that annoy us, but which really do not matter in the broader context. And so, we continue to fall into the same patterns of behavior that we have tried previously without ever making real progress on the problem.

The key to an effective cyber security program is to agree on what the Goal is. What is the Goal of the security program? To stop the "bad things." There are "bad things" that can happen, and security should either prevent these "bad things" outright or lower the impact if the "bad things" do happen.

QUESTION 2:
HOW SHOULD I APPROACH MY CYBER SECURITY GOALS?

In two words "Risk Management".

Risk Management is a very large topic, and we don't have time to give it proper treatment now. Suffice to say, if your security program does not look at things through a Risk Management lens you will have a tough time reaching the Goal. Let's take a look at a "bad thing" from a Risk Management perspective.

FROM THE PRIMARY STAKEHOLDER PERSPECTIVE

This is specifically from the OpenFAIR [1] approach to risk management, but other risk frameworks handle it similarly. You have threats (hackers, insiders, nation states), who are trying to breach your assets (information, databases, etc.). If they succeed there is a loss event (breach or incident) that causes both direct consequences (pay for response, lost productivity, etc.) and reactions from others (lawsuit, regulator, loss of reputation).

[1] WHAT IS OPEN FAIR™ AND WHO IS THE OPEN GROUP? (FAIRINSTITUTE.ORG)

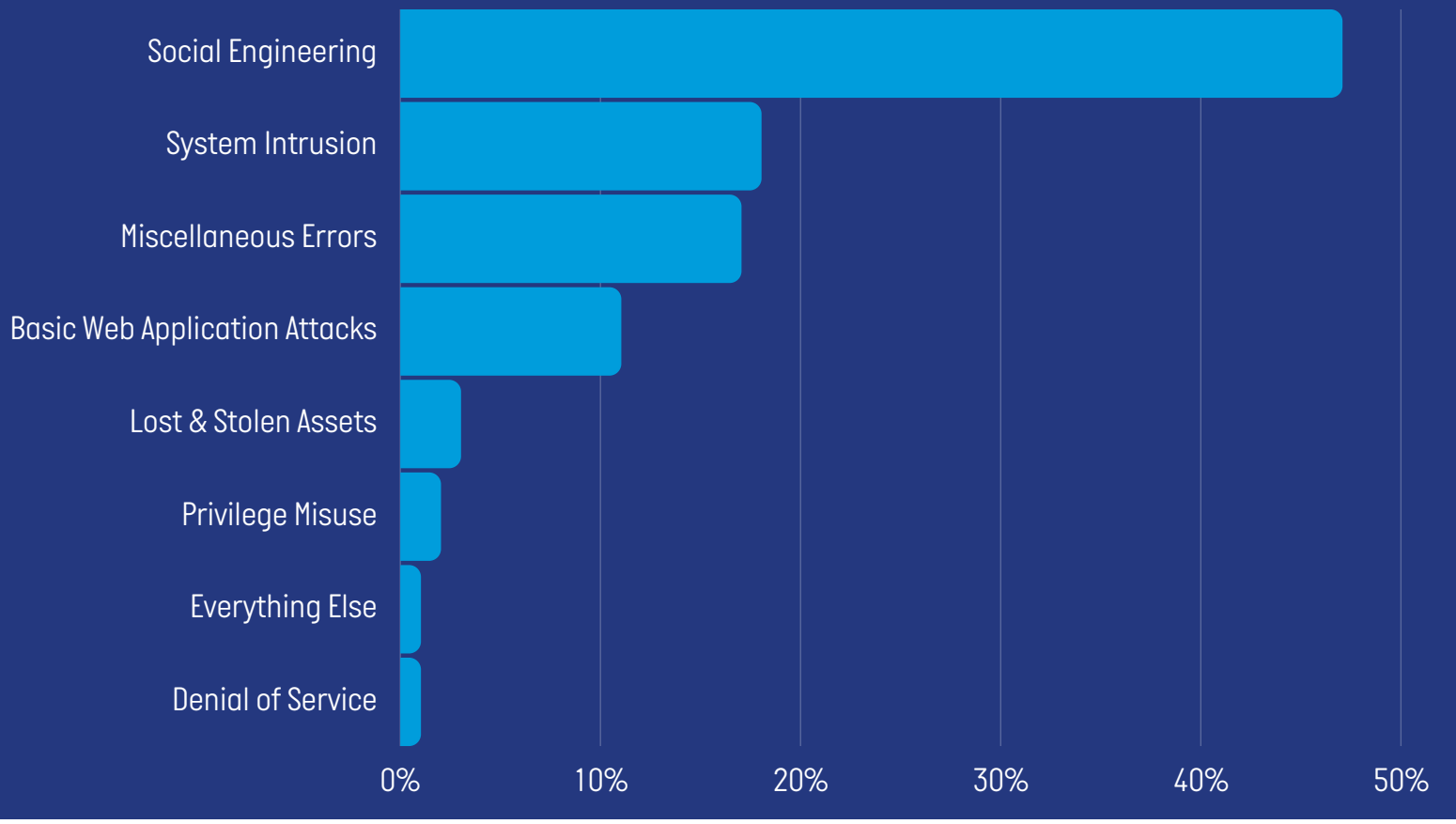
So far, we've been pretty generic in our discussion. How does it effect you directly? Wouldn't it be nice if you could have an idea about what “bad things” you face and then focus your efforts appropriately? Fortunately, there is very solid and useful information published annually in the Verizon Data Breach Investigation Report [2]. This report breaks down the "bad things": who does them, how they do them, and their motivations. This is further broken out by business vertical. Very helpful since what is happening in retail is not necessarily applicable to manufacturing.

Let's take a look at the higher education space and see what "bad things" have been happening lately.

[2] HTTPS://WWW.VERIZON.COM/BUSINESS/RESOURCES/REPORTS/DBIR/

QUESTION 3:
WHAT SECURITY THREATS DO I NEED TO WATCH OUT FOR?

FIGURE 1 - ATTACK PATTERNS IN EDUCATION BREACHES



What this chart shows us is that social engineering attacks account for approximately 45% of all breaches in the education space. With system intrusion (hacking), miscellaneous errors (employee fat finger mistakes), and web application attacks rounding out the top 4.

QUESTION 4:
BUT HOW DO I ADDRESS THESE SECURITY THREATS?

Now that we've touched on what "bad things" we should be worried about, how do we address them? Fortunately, the Data Breach Investigation Report provides some recommendations for which of the Critical Security Controls [3] would be most helpful. Let's focus on what could help with Social Engineering as an example.

In order of effectiveness and impact here are the top 5 security things you should do:

1. ACCOUNT MANAGEMENT

Assign and manage authorization for users, including administrator accounts and service accounts, to enterprise data and software.

2. SECURITY AWARENESS & SKILLS

Have a security awareness program to influence behavior to be security conscious and skilled in reducing cybersecurity exposure.

3. INCIDENT RESPONSE

Develop and maintain an incident response capability to prepare, detect, and quickly respond to an attack. This would include policies, plans, procedures, defined roles, proper training, and communications.

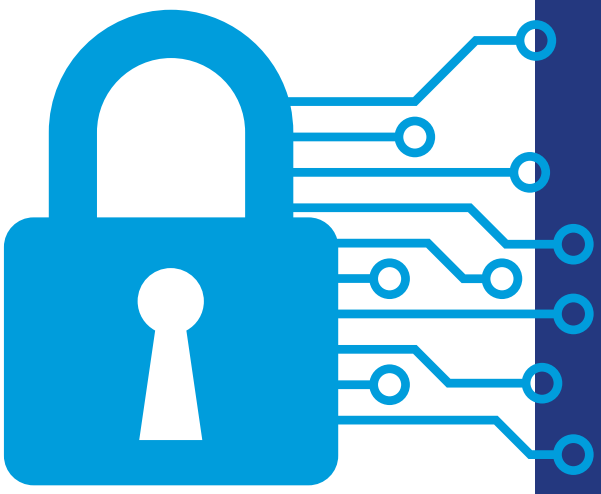
4. ACCESS CONTROL

Create, assign, manage, and revoke access and privileges for users, administrators, and service accounts for enterprise data and software.

5. AUDIT LOGGING

Collect, alert, review, and retain audit logs that could help detect, understand, and recover from an attack.

[3] HTTPS://WWW.CISECURITY.ORG/CONTROLS



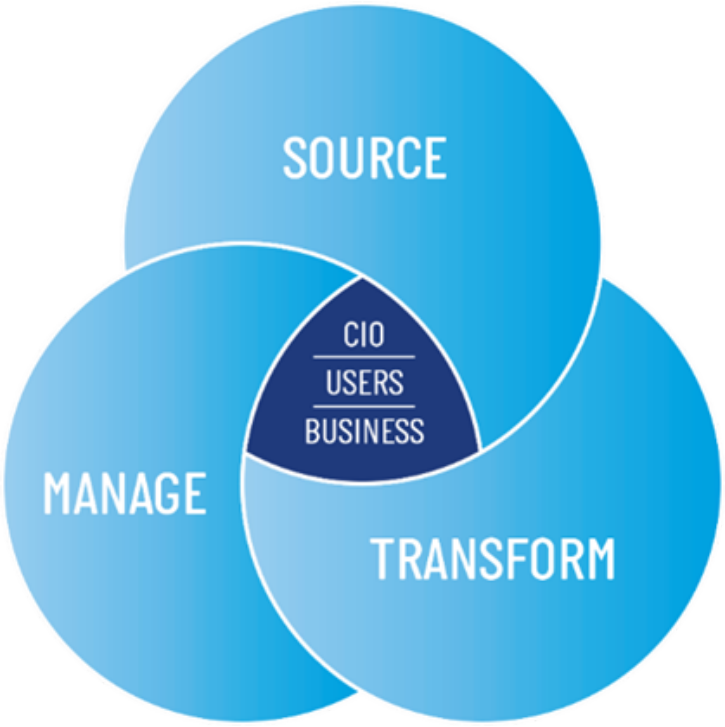
SECURITY CONTROLS CONT.

Even limiting this to the top 5 it is daunting list. However, you can also see that some of the controls complement one another. For example, account management and access control fit together nicely into identity management as a whole. Access control feeds into audit logging. And audit logging complements incident response. There are no clear boundaries between the controls, and that can make it all a bit overwhelming.

QUESTION 5:
HOW CAN I BUILD A ROAD MAP TO ACHIEVE MY CYBER SECURITY OBJECTIVES?

This is where CCTM can help. Once we've helped you identify what your primary concerns are, our architects will work with you to come up with a high level reference architecture, using our Source, Manage and Transform approach.

FIGURE 1: We help our customers to Source, Transform and Manage their technology infrastructure, to deliver digital transformation, enabling people and their business



SOURCE: TECHNOLOGY SOURCING

We help our customers to determine their technology needs and supported by our Technology Partners, we arrange the commercial structures, integration, and supply chain services to meet them reliably.

TRANSFORM: PROFESSIONAL SERVICES

We provide structured solutions and expert resources to help our customers to select, deploy and integrate digital technology to achieve their business goals.

MANAGE: MANAGED SERVICES

We maintain, support, and manage IT infrastructure and operations for our customers to improve quality and flexibility while reducing costs.

What you're left with is a reference architecture and plan to address the real issues that are facing your institution. You can demonstrate meaningful tangible risk reduction and security improvements. Time to stop chasing your tail when it comes to security.

Our team of IT experts can help answer your most pressing cyber security questions, give your organization peace of mind with cyber security services from Computacenter.

Connect with our cyber security experts today +1 (647) 333-6241

WHO WE ARE

COMPUTACENTER

Computacenter TeraMach, Inc. (CC TeraMach) has over 24 years of experience in the public sector, education, healthcare, and commercial industries, focusing on Digital Transformation in the areas of Security, Cloud, and Edge. Our extensive data centre technologies' experience, digital services capabilities, strong vendor relationships, and deep technical knowledge has enabled us to be the trusted partner for our 2000+ satisfied customers.

Computacenter is a leading independent technology partner, trusted by large corporate and public sector organisations. Together, we help our customers to source, transform and manage their IT infrastructure to deliver digital transformation, enabling people and their business.

WHO YOU'LL CONTACT

JASON MURRAY
SOLUTION ARCHITECT AND TRUSTED ADVISOR

PROFILE

Jason is based out of Toronto and is passionate about solving security issues within the Educational space.

EXPERIENCE

With more than 20 years of experience in the technology sector Jason has the technical skills to support your business in achieving their digital transformation goals.

Connect with our cyber security experts today

+1 (647) 333-6241