The IT Mill

Like Newsletters Should Be.

Fall 2021

Business

What Is Your Chocolate Cake Recipe?

By Scott Birmingham, Principal Consultant, C.E.T., C.I.M.

Earlier this year, we completed our annual planning process here at Birmingham Consulting and it had us reflecting on our recipe for chocolate cake. You may be asking "What does chocolate cake have to do with IT?" Bear with me...

I learned about this concept a few years ago; and after revisiting it internally, I thought I would share it. So, let's start by considering just how many different types of chocolate cake exist:

- Mass-produced in a factory and shipped to stores.
- Basic commercial bakeries found in grocery stores.
- Premium commercial bakeries that sell to restaurants.
- Privately-owned bakeries open to the public.
- Special request bakeries (i.e. gluten-free, dairy-free, etc.)
- The list goes on...

Are all of these cakes the same? Do they all taste the same? Sell for the same price? If not, why not? They all typically contain the same basic ingredients: Coco powder, flour, sugar, and/or eggs, oil, milk, etc. What makes them different? Why does a mass-produced cake have a different taste and price than a custom-made cake?

If your product or service was chocolate cake, why would your cake be different? Is it price? Quality? Service? Speed? Intellectual property? Experience? Combinations thereof? Something else?

And now a tough question: **If your competitors were asked the same question, would it sound a lot like your answer?**

There is an actual marketing term for this concept: Unique Selling Proposition (USP). Depending on who you ask, there are different ways to create a USP. Two common ones are:

#1 - Identify 6-8 things that set you apart from the competition. Your competitors may be able to claim some of the same things; but they can't match all of them.

#2 - The "3 Uniques". Similar to above but you only identify 3 things that make you unique compared to competitors – they might be able to match any 2 of them; but not all 3.

We'll wrap up with another tough question: *Is there ONE thing that sets you apart from your competition – something that nobody else can claim?* (Don't panic if you don't have "The ONE Thing" – not everybody does.)

If you haven't already performed this exercise, I encourage you to do so and plan to revisit it annually.

What Is Our Chocolate Cake Recipe?
Visit birmingham.ca/like-it-should-be to learn about our proven recipe and why we're the IT company people actually like to talk to.™

BIRMINGHAM CONSULTING
Like IT should be.®

21 Mill Street North
Waterdown, ON
L0R 2H0

(289) 895-8948

www.birmingham.ca
info@birmingham.ca

Security Discussion

How Much Should You Invest In Cyber Resilience?

(Hint: It's Different Than Your IT Budget)

By Scott Birmingham, Principal Consultant, C.E.T., C.I.M.

There's been a lot of talk recently about large ransomware events (e.g. Colonial Pipeline, JBS Foods). The disruptions felt by many people, millions demanded, and articles made top news. One article stood out for me. The author questioned how much money companies were investing in cyber resilience compared to the ransom payouts.

Using the $4M Colonial Pipeline ransom as an example, they posed the hypothetical question of whether they wish they had invested an additional $4M to prevent and/or recover quickly from an attack that shut down production.

Many experts opine that not enough is being invested in cyber resilience; but there's little practical information on how much is the "right" amount. When does the investment reach the point of diminishing returns? Couple this concern with the tendency for businesses to underestimate both the threat level and impact of a cyber event - the result is often too little invested, too late.

So, how do you determine a realistic amount to invest? $4M is a lot; but is it a lot to Colonial Pipeline? Colonial's annual revenue is approximately $500M/year; $4M translates to about 0.8% of annual revenue.

Looking at some of the top non-governmental and non-healthcare ransom payouts over last 12 months: average ransom was 0.22% of annual revenue. But this is only a fraction of the total cost: legal, remediation efforts, downtime, lost business or lost client confidence, increased liability, etc. add up considerably.

If a $25M/year business experienced a ransom event, at 0.22% of revenue, they could expect a ransom demand of $55,000. That's before adding in the related costs listed above. **Would it be worth increasing your investment by that same amount annually to eliminate the problem; or even to significantly reduce the impact?**

If your answer is "no", then stop reading. But if "yes", ask yourself how to best improve your cyber resilience and get the most return on that additional investment.

Business is dynamic. Threats are dynamic. Diligent business leaders understand this and ensure that their cyber resilience strategies stay aligned with changing environments.

A final thought as a disclaimer: This article is not intended to provide any kind of legal or financial advice. Every business situation is unique. The intent is merely an attempt to provide a quantified reference point for what is often a nebulous topic in the world of technology.

Shameless Self-Promotion

Newest Team Member Spotlight: Yll Konjufca

By Yll Konjufca, Technology Associate

Yll and his dog, Argo

I graduated in Computer Science and worked in the IT industry for about 5 years in Kosovo before moving to Canada to pursue dreams and enjoy the different challenges that life brings.

Since IT is a fast-moving industry, updating my skillset through schooling and certifications prepared me better for the Canadian market. After having some experience here, I joined the BCI team; which brought me to a whole new chapter professionally.

What's great about being a part of the team here is that the staff are not just 'work colleagues' but people that you can rely on, share good and bad news, and individuals that foster a family spirit. I haven't seen this anywhere else in my experience – Mondays just feel different here.

The motivation to be a techie came through the idea of the endless possibilities that technology offers. However, after I started working in tech, I realized that one of the great things I like about IT is that it runs on strict protocols, giving you instant feedback - there's no way around it. Thus, the only option left is doing things correctly (because you can't argue with 1's and 0's).

One of my favourite things about working at BCI is that there's no compromise in the quality of work; it should be done in the right way with attention to all details. Another favourite thing is their value of standardization - which to me as an employee gives me the confidence of being on the same page with everyone on the team, and also offering the ultimate product and care to all of our clients.

"Quality, Integrity, Partnership"

AIRMAX COMPRESSOR SERVICES

"Our relationship with Birmingham Consulting is a ***true partnership.*** They take the wellbeing of our business as seriously as we do. The few issues that do occur are resolved **expediently** and **professionally**. With Birmingham, **quality, integrity** and **delivery** are second to none."

- David Wharton, Airmax Compressor Services

Technology

The Slippery Slope of Employee Activity Monitoring

By Christina Birmingham, HR & Finance Manager, C.H.R.L. & Scott Birmingham, Principal Consultant, C.E.T., C.I.M.

DISCLAIMER: We encourage any employer who may be considering implementing employee activity monitoring to first consult both with a certified HR professional and lawyer familiar with both employment and privacy legislation.

U.S. law and Canadian law differ significantly when it comes to both privacy and employment. The bulk of information available online is from U.S. sources and is only relevant to the U.S. employment market. For Canadian employers, locating information on this topic can be difficult; so we urge caution when conducting online research.

With all of the disclaimers out of the way, on to our topic. Within the last year of the COVID pandemic, we've received more inquiries about monitoring employee activity than we did in 10+ years prior to the pandemic. Coupled with this increased interest from employers, it seems that every month, trade publications have articles related to monitoring employee activity.

Despite all of this interest, not one of our clients has implemented employee activity monitoring. If you're an employer, you might be wondering "Why not"? Bottom line is that there are both pros and cons to monitoring your employees' activity. Usually, the cons outweigh the pros.

Most people think that all pros would only be for the employer because they can track employee utilization, actual hours worked, whether staff members are viewing job postings, uploading information to unauthorized locations, audit trails, etc.

Though maybe not obvious, there are some pros for employees as well. One of the biggest pros is assisting with demonstrating issues that might not otherwise be captured (for example, intermittent or unique technical problems). Logs will also provide confirmation of work done if something happens to go missing and metrics to warn if you're working too much.

But before an employer rushes out to implement the latest monitoring platform, consider the top three reasons our clients have, after fully exploring it, opted to not implement it:

#1 **Privacy.** In Canada, courts have ruled employees have an expectation of personal privacy even when using company-owned devices. Implementing monitoring without consent could be a violation of privacy rights.

#2 **Security.** Monitoring systems contain confidential information; both business-related as well as employee personal information. If that system is cloud-based, how secure is it? In what country does the data reside? (i.e. does it comply with Canadian legislation?) Does the service include a backup or must that be implemented separately? Etc.

#3 **Erosion of culture and trust between employer and staff.** When an employer is trying to foster a "team" atmosphere, employees often consider monitoring to be a sign of mistrust and contradictory to a "team" culture.

All of this is not to say you shouldn't implement employee activity monitoring. However, the first inquiry shouldn't be with IT and the technical viability. The bigger challenges to overcome will be with HR and legal compliance. Once those areas have been addressed, then start evaluating technical solutions to provide the information you're looking for.

Community

100+ Women Who Care Flamborough-Waterdown

Save the date to join the next meeting on Wednesday January 19, 2022, 7:00pm - visit www.100womenflamborough.ca to learn more and pre-register.

Our local Flamborough-Waterdown chapter of 100+ Women Who Care brings together 100 (or more) women who care about local community causes and who are committed to community service. At the online meetings, a local charity or not-for-profit organization will be jointly selected. Everyone each donates $100 to the selected organization and watch how the group's commitment turns into a $10,000+ donation. Do that four times a year and witness how $40,000 can improve the lives of our neighbours.

Kahn's Korner

You can tell by his expression that our honourary Health and Safety Rep, Kahn, takes our team's safety seriously.

Client Spotlight

ele-com electrical services

Ele-Com Electrical Services Inc.

www.ele-com.ca *(905) 538-8001*

Ele-Com started in 2010 as an electrical and telecommunications contractor and has recently added security cage design and build to their portfolio.

The owners, John Weinrich and Jane Davidson, combined their skill sets, John's technical skill and expertise plus broad base of construction knowledge with Jane's operational skills and experience, to form an electrical contracting company.

They work primarily with commercial customers on a variety of construction and maintenance electrical and telecommunication projects. Over the years, they have built a strong core of expertise and skill sets including much in-demand fiber repairs and are known for being a one stop shop for projects; with their services including post construction clean up repairs and refinishing.

Their teams are motivated by the desire to ensure their customers are satisfied with every project they work through. They partner with their customers on each project, provide recommendations, and work closely with them to identify and resolve any project roadblocks.

COVID paused their team fun, but when they are out of lockdowns and restrictions, they will continue their "Bay Door BBQ's".

Partner Spotlight

datto

Datto, Inc.

Our Like IT Should Be® Toolbox

When we evaluate a company's offerings, we place the value delivered to our clients above cost. There's no point in saving a few bucks at the expense of clients being underserved.

Datto fits squarely into this category. Despite evaluations of competitive solutions, we have yet to find anything better than their flagship products: Business Continuity / Disaster Recovery (BCDR) and Cloud Account Protection.

From a business standpoint, the Canadian market is not just an afterthought for Datto. For many tech companies, Canada is viewed as an extension of the U.S. market. But Datto has a strong Canadian presence; both in staffing and technology. They are committed to Canadian "data sovereignty" – keeping Canadian data within Canadian borders.

Why Datto For Our Clients? Here's An Example:

After receiving an overnight alert that a client server was offline, we arrived onsite before start of business and diagnosed a hardware failure. The server was under warranty; but we would have to wait until next business day for the manufacturer to repair. Thanks to Datto BCDR, we had the client fully functional within ½ hour of arrival. The best part is that except for our client contact, ***nobody even knew there was a problem.***

Interactive Infotainment

Which of these statements is FALSE when it comes to Small-Medium Businesses and Cyber Resilience?

Submit your answer online at **BIRMINGHAM.CA/QUIZ** by October 31, 2021 for a chance to win a Tim Hortons gift card!

- **A.** 63% experienced a breach in the last year
- **B.** 20% don't use any endpoint protection (aka antivirus)
- **C.** 43% lack any type of cyber resilience plan
- **D.** 4% employ advanced / enhanced protection
- **E.** 60% think their business is not being targeted

Thank you to everyone who participated in our last quiz: the best reason to use a VPN was answer B. - Keep your data private.

BIRMINGHAM CONSULTING
Like IT should be.®

21 Mill Street North
Waterdown, ON
L0R 2H0

(289) 895-8948

www.birmingham.ca
info@birmingham.ca