Forbes Insights

PROTECTING YOUR PASSION

CYBER RISK AND SMALL BUSINESS

IN ASSOCIATION WITH: Symantec
CONTENTS

Introduction..........................................................................................................................2

Passion at the Core ...............................................................................................................3

Case Study 1: Better Safe Than Sorry................................................................................4

Case Study 2: Preserving a Legacy......................................................................................6

Case Study 3: Playing for Profit..........................................................................................8

Case Study 4: A Cybervault for Boutique Bankers..............................................................10

Lessons Learned From Those Protecting Their Passion..................................................11

Acknowledgments.............................................................................................................12
INTRODUCTION

Entrepreneurs would rather concentrate their efforts on growing their businesses than on managing the tactical yet important tasks of staying compliant, managing talent, arranging financing and attending to information technology needs. Ensuring that these critical backbone requirements are taken care of is crucial if a company is to stay competitive, productive and trustworthy—in other words, to be successful in the marketplace. How do company owners make this happen without taking their eyes off the core business?

To help answer this question, we interviewed 11 entrepreneurs of very small companies in seven countries across a range of industries. We asked them about the risks they face and how they manage those risks, particularly Internet security and data protection. Not one was entirely confident that his or her safeguards were adequate. Most have pieced together defenses that they recognize will need to be enhanced if their firms continue to grow.
PASSION AT THE CORE

At the core of every small business is passion.

In the case of Lumos Learning, that passion is education. The Lumos e-learning platform and workbooks help students do better in school and on standardized tests: students work interactively with teachers, take practice tests or just get a little help with math and language concepts. Mukunda Krishnaswamy started Lumos five years ago after buying his nine-year-old son Vivek expensive test preparation software, only to discover the content had nothing to do with the test administered by his local school district.

Krishnaswamy worked with Vivek’s third-grade teacher to create practice tests that mirrored the standardized exams administered in his hometown of Piscataway, New Jersey, in the United States. They gave the test away for free to anyone who wanted it. “We got a great response from students as well as parents about how useful these tests were,” he said. “They wanted more.”

He pooled his savings with another partner and collaborated with local teachers to design an interactive database as well as printed books and software for teachers. His timing was fortunate. Most states, including New Jersey, have agreed to adopt the Common Core State Standards, an initiative to provide teachers and students with a consistent blueprint and basis for testing what every student is expected to know after completing each grade. As states begin the transition to the Common Core over the next few years, Lumos has the potential to greatly expand its geographic coverage.

Lumos has already expanded the sophistication and technical complexity of its offerings beyond the practice tests passed out for free in 2007. Teachers and parents can use a dashboard to view progress, assess weaknesses and even create custom lessons. Products range in price from $5 for 48 pages of reading comprehension activities and practice tests for a third-grader to nearly $3,000 for a one-year library subscription with full-length practice tests for grades three through eight. More than 13,000 students use Lumos products, some purchased by parents, some through the 160 schools and 26 libraries that use Lumos materials.

The company now has seven full-time employees and a network of around 30 contributors—mostly teachers working over the summer. Even Vivek, the son who inspired the creation of Lumos, has gotten involved in the business after taking second place in an elevator-pitch contest for a new product: Lumos Writing Zone, a composition tool that enables students to generate ideas interactively, expand their essays and work collaboratively.

Krishnaswamy started with one advantage. He spent much of his career developing and implementing enterprise applications, most recently as chief technology officer at American Standard, a company with $11 billion in annual revenue before it was split up in 2007. He is more aware of the value and the risks of doing business online than most small-business proprietors.

Without a reliable website, Lumos wouldn’t be in business. All of its teaching products are interactive; even the printed booklets come with online access for practice tests and answer keys. “We are completely dependent on the Internet,” says Krishnaswamy. “And we are dependent on architecture provided by other players,” he adds. Lumos relies on off-the-shelf products, such as Google, Microsoft Outlook and PayPal. As a techie himself, Krishnaswamy knows enough to make sure all sensitive personal data is encrypted and credit card numbers are not stored anywhere on his servers. In addition, he runs a program called Copyscape to ensure all the material on the Lumos site is original and to look for illegal use of Lumos content by others.

“We’ve been lucky so far, but we are looking for partners that have the expertise to monitor our website for suspicious activity.”

—MUKUNDA KRISHNASWAMY
Founder, Lumos Learning
CASE STUDY 1: BETTER SAFE THAN SORRY

JIM BETLAND, Challenge Machine and Manufacturing, Blaine, Minnesota, U.S.A.

Jim Betland started Challenge Machine in his garage 14 years ago, but the equipment he owns looks like it would be more at home in a science lab. Each machine has its own desktop monitor to control the robotic arms and spindles that carve precision parts. Some of the micro components his engineers crank out look like tiny square jewels, too small to pick up with bare fingers.

The machines are not that special, he insists. The real challenge is finding good people. Challenge Machine has doubled in size nearly every year since 1999. Betland just hired three more employees, bringing the total to 19, but he worries that candidates will become even harder to find as his company continues to grow. “Schools are eliminating shop classes,” he says. “Most people think this is a dark and dingy business. But the machine industry has done a good job of eliminating oil.”

Betland’s customers are looking for bespoke parts: pieces to outfit medical equipment, sockets for semiconductor manufacturers, prototypes requested by universities. “We aren’t always sure what the parts are for,” says Betland. The mystery may be intentional, as in the inner components for airport scanners that Challenge supplies.

Because of the proprietary nature of customers’ designs, Challenge employees must upload them through a secure file-transfer protocol (FTP) site set up by each client that allows access only to areas of the site that contain design instructions for Challenge. Workstations that access customer data do not have unrestricted access to the Internet.

“Everybody had a different idea how to fix it.”

—JIM BETLAND
Founder,
Challenge Machine

“We used to be more open, and we were running into all kinds of problems,” says Betland. “Everybody had a different idea about how to fix it. We just kept throwing money at the problem, but all it would take would be one person checking football scores and downloading a virus,” he says. “Everything we put on to stop it slowed us down.”

As annoying as it was to clean up infected computers, Challenge faced a threat far more serious eight years ago when someone hacked into the company network. The hacker seemed to know what to look for. “It had to be someone very close to the company,” says Betland. “There were multiple attempts to get into sensitive areas. They didn’t get anything, but they probably would have with a little more time.”

Now Challenge has only a couple of computers that have open access to the Internet, and they do not run on the same server that connects to clients. Betland has also shut down the wireless network inside the building after taking a few malicious hits. “No one outside this building can get access to our sensitive data, unless they take it out on a USB,” says Betland.

Even the desktops now connected to the Internet are covered by greater security, but they are far from maintenance-free. “We found we were being blacklisted on a number of servers,” says Betland, “including Symantec’s.” It turned out that not all of Challenge’s software was updated with the latest patches—a problem that was easily fixed by the IT specialist Betland contracted.
The virus infected both sides,” he says. “It shut us down for a few days.”

—KEVIN FLANAGAN, Co-Founder, Custom Packaging Supply

Not all Internet security violations end in disaster. Most are the kind of trivial annoyances that eat away at productivity and patience. All it takes is for one employee to download a virus and hours of work might be lost chasing down a fix. For companies operating on a shoestring with only a few employees, having one person down can be a major disruption. Having a whole system down can be a disaster. Kevin Flanagan, co-founder of Custom Packaging Supply in Camarillo, California, in the U.S., discovered this the hard way.

Custom Packaging Supply designs corrugated boxes for consumer products, medical supplies and manufacturers. The company then outsources production before distributing the final orders to customers. Flanagan knows packaging. He studied it in college and worked at a larger packaging company for six years until 2006. As the economy went into a tailspin, container manufacturers began cutting back on package design. That’s when he saw an opportunity. He quit his job and together with a partner set up Custom Packaging Supply as a design and distribution company. The company generated revenues of $10 million last year and now has 18 employees.
Rasha Shehada learned about risk at an early age. Her grandparents escaped the ravages of war in Palestine, and her father, Kamal Shehada, eventually moved to the UAE. He started a small trading company in 1997 supplying the Emirates’ hotels, but he had bigger goals. He was determined to provide a legacy for his family that would give them financial stability. His opportunity came when one of his suppliers ran into trouble in China.

The supplier, a broker of towels, tissues and housekeeping supplies to the world’s hotels, was desperate to pull out of an inefficient and outdated joint venture in China that made chafing fuel, the stuff that keeps serving trays warm at hotel banquets and buffets. But closing down a factory in China was not easy at the time. First, there would be a penalty to pay the government, and then there was a requirement to pay workers’ wages for five years after closing. Shehada offered to buy the factory, but the supplier said he could have it for free if he would deal with the regulators in China.

Shehada managed to convince Chinese authorities to allow him to close the factory in return for providing employment to the workforce in a new factory in the UAE. He offered two-year contracts to 10 Chinese employees to work in Dubai with the opportunity to learn English and see something of the world outside the People’s Republic.

“Everything is online except the factory.”
—RASHA SHEHADA
Managing Director,
Diamond Line

Shehada estimates she spends 90% of her time online. All of the company’s accounting and delivery software, most communications with customers and employees, and all documents for Dubai’s paper-free bureaucracy are web-based. “Everything is online except the factory,” says Shehada.

As a manufacturing company without an active website, IT has not been a focus for Diamond Line. “I am not a tech person, and we don’t have an IT department,” says Shehada. But the firm is reliant on the Internet for much of its business. Shehada estimates she spends 90% of her time online. All of the company’s accounting and delivery software, most communications with customers and employees, and all documents for Dubai’s paper-free bureaucracy are web-based. “Everything is online except the factory,” says Shehada.

“Five years ago, I would have said we don’t need to waste our money on consultants,” she says. “But I hear more and more about how small- and medium-size businesses are being hacked.” Employees use over-the-counter antivirus software on each individual device, and the company hired an outside service to run a firewall. “It’s too hard to do on our own,” says Shehada.
Every design begins with a computer-assisted design program. That application controls a digital cutting table that slices through corrugated sheets to create a template and sample that can be sent for production. Without a functioning computer system, the firm’s two design engineers can’t work. Neither can the salespeople, the finance department, the warehouse workers or Flanagan. He thought that risk was mitigated because the firm’s one hard drive was mirrored, meaning it was replicated byte-by-byte in real time. Not so. “The virus infected both sides,” he says. “It shut us down for a few days.”

The company brought in an outside consultant, who deployed stronger security and ended up saving the company some money by using a cloud-based service to back up data, thus avoiding a server upgrade. Compared with losing a few days of work and a lot of data, “hiring another company to run our security is extremely cost effective,” says Flanagan.

Virus protection software might hold off some attacks, but it requires regular maintenance. Most of the companies we approached began with whatever anti-virus software came with their desktops and other devices. As they added employees, each piece of new equipment came with its own software and licensing agreement. By the time there are a dozen or so computers, the task of renewing licenses and updating software can become a real drain on someone’s time. At Eiger Securities in London, that someone was Richard Ashton, senior partner at the 40-person bond-trading boutique and IT firefighter by default.

Ashton established the Eiger Group a decade ago with a group of fellow traders. Traders at Eiger Securities buy and sell government debt, corporate bonds and other fixed-income products for banks, hedge funds and insurance companies throughout the world. Another part of the group, Eiger FX, handles currency transactions at better rates than most companies can obtain from their banks. “Small differences can add up if you are trading millions of dollars,” he explains. Transactions are processed through electronic trading platforms, but finding buyers and sellers, discussing bids and offers and negotiating deals, are all done by phone and email. Even in a negotiated trade, speed matters.

“Small differences can add up if you are trading millions of dollars.”

—Richard Ashton
Senior Partner,
Eiger Securities
CASE STUDY 3: PLAYING FOR PROFIT

PETER MORRISON, Bohemia Interactive Simulations, Prague, Czech Republic

A gaming software developer, then called Bohemia Interactive Studio, was started in the Czech Republic in 1999 but took on a new life when an enterprising Australian saw the possibility of using the software for virtual military training exercises. He worked with the Czech developers to create a program that proved a hit with military trainers in Australia, Europe and North America.

Peter Morrison was an officer in the Royal Australian Signal Corp at the time, specializing in military simulation. He began working with Bohemia Interactive in 2005 as a contractor and eventually became lead developer of a more dynamic version of the company’s flagship product: Virtual Battlespace 2. The Australian government purchased an enterprise license for A$2.5 million, and Morrison put together a team of “friends from the Internet,” to work on development. Most of them were already working together in “mod teams,” players who modify games by creating new 3D models and terrains or improving the game’s artificial intelligence. The first time he met most of them in person was when they accepted their job offers. “It’s a company built on a hobby,” he says. The original team of 10 worked closely with the U.S. Marine Corps and the Australian Defense Force to create battlefield scenarios that can be customized to include ground clutter, animal life, weather and dynamic lighting.

The company, now known as Bohemia Interactive Simulations, does a majority of its business with the U.S. military. Morrison, who is now CEO, spends a lot of his time in the U.S., especially in Orlando, Florida, where the U.S. Army and Marine Corps have procurement offices.

Having the U.S. military as your primary customer poses certain risks for a vendor that is based overseas. “Military data has restrictions,” Morrison explains. Sending data to Bohemia Interactive’s programmers in the Czech Republic requires clearance, for example. “We spend a lot of money on lawyers and consultants to make sure we comply with ITAR (International Traffic in Arms Regulation),” says Morrison.

Still, export controls can be managed, he adds. Finding enough qualified software developers, training them and keeping them is more difficult, he says. “It’s a competitive market, and big companies are always hiring.” The first 10 employees are still with the firm, he says, but Bohemia Interactive is expanding fast. Earlier this year, the firm received private equity backing from the Riverside Company, a U.S. investment partnership.

The firm’s biggest risk, however, is keeping its source code safe. “We have a huge library of content,” says Morrison. All of Bohemia Interactive’s data is encrypted, but “any software can be hacked,” he says. “We spend a lot of time monitoring the Internet to make sure our data isn’t out there.” Sometimes, it is. The firm had to take legal action when monitors found elements from the company’s 3-D art library for sale on a computer model marketplace.

Even with all those geeks on the payroll, Bohemia Interactive relies on consultants for data backup. “We thought we could do it ourselves, but everything was substandard,” says Morrison. “I look back at our early years and shudder. The entire value of our company is in our intellectual property. We were so lucky.”

“I look back at our early years and shudder.”
—PETER MORRISON
CEO, Bohemia Interactive Simulations
Not only was Eiger’s off-the-shelf antivirus software in need of constant attention—one workstation at a time—but traders were complaining the constant virus scanning was slowing down their systems, too. “It seemed like every application and update became ever more processor-hungry,” says Ashton. He brought in an outside consultant, who shifted Eiger’s workstations to a centrally managed system and also relieved him of backing up the years of data that UK and EU regulators require securities dealers to keep.

Eiger now employs three full-time IT specialists, says Ashton, mostly to safeguard against the more serious risks faced by the firm: fraud, theft of financial data and compliance related to anti-money-laundering regulations.

For most proprietors, Internet security is only one of many risks they face every day. In fact, nearly everyone we interviewed mentioned hiring and keeping good people as the top risk to their business. Most expressed concerns about the potential damage a careless or malicious employee could do—everything from theft to fraud.

Small medical practices may be particularly vulnerable. One reason: doctors and dentists are not known for their business acumen, says Hisham Barakat, a dentist by training. He left a large established dental group where someone else took care of everything from answering the phone to filing insurance claims to keeping the lights on.

Now, after buying four existing practices from retiring dentists, he finds himself splitting his time between seeing patients and running his combined practice like a business. Technology has helped. With the aid of IT consultants who specialize in dentistry, he has moved every function he can online, from scheduling appointments to working with laboratories that design crowns and implants for his patients. With only 14 employees, “it would be crazy for us to try to do this in-house,” he says. At the end of every day, an IT consultant backs up the database and runs regular checks of his firewall, freeing up time for the doctor to keep an eye on his dashboard of patient appointments, treatments and follow-ups.

His biggest concern: fraud and embezzlement. “Three out of five dentists are victims of embezzlement,” he says. It gets worse. “I was an expert witness in the case of another dentist,” he says. Not only had the defending dentist been embezzled by his office manager, but someone had used his name to write fraudulent prescriptions for narcotics. “He was sentenced to two years in prison for something he didn’t do because he had no proof,” says Barakat. Having practice-management software in place helps to leave a cyber trail. But to make sure he is fully aware of what takes place in his office, Barakat is beta-testing software that sends him a text every time there is a transaction connected to his practice.
CASE STUDY 4: A CYBERVAULT FOR BOUTIQUE BANKERS

PANKAJ THAPAR, IndoStar Capital, Mumbai, India

IndoStar Capital may be a tiny start-up, but it’s backed by some powerful investors: Goldman Sachs, Baer Capital Partners, the Ashmore Group and China Development Financial, among others. The big guns backing IndoStar reach around the globe, but the firm’s business is strictly local. The Mumbai-based boutique was established two years ago with $200 million in capital to lend rupees to Indian companies.

Think of IndoStar as a private debt investor with a business model similar to private equity: targeting certain industries and making sizable, leveraged, hands-on deals through debt rather than equity. “Everybody does equity,” explains Pankaj Thapar, one of the firm’s founding executives. The firm’s backers saw an opportunity to invest in India’s growing debt market with a small group of experienced bankers by creating a lender more specialized than India’s big commercial banks.

Most of IndoStar’s 27 employees specialize in evaluating credit risks, creating structured debt products and keeping tabs on the debt IndoStar has extended. With so little support staff, Thapar himself wears more than one hat. He is both the CTO and the CFO, responsible for protecting the firm’s finances as well as its data. “If you don’t use technology, you will keep adding headcount and suddenly find you have too many people,” he says.

What keeps him awake at night is credit risk: what might happen to companies to whom IndoStar has extended credit. Because IndoStar is underwriting individual loans as high as $30 million and leveraging its capital, any trouble experienced by its customers will be trouble for IndoStar. “We are always watching our customers’ business areas, monitoring our credit risk and thinking about how we can diversify our portfolio,” he says.

One risk he does not want to worry about is data protection. Part of the firm’s network is as open as that of any other small business: employees can log in to the firm’s mail servers from outside and also do basic industry research over the Internet. But once a deal is in the works, the documentation is handled offline. “With a structured loan, every transaction is unique,” explains Thapar.

When a deal is completed, full security kicks in. The information is stored in a database segregated from any Internet connection. “Our lending database is extremely secure,” Thapar says. To overcome the possibility that someone might tamper with lending and repayment data, he has put the back end of IndoStar under “lock down,” as he describes, with a visible trail for changes made. “The only way to access the database is from inside the company, on a company device, and I am monitoring real-time,” he says. Access to external drives is disabled, and only a few people are authorized to download anything on a CD or USB drive.

“It’s easy for me to mandate access now,” Thapar says, “but I’m not sure if it will work in a few years or if we open an office in another city.”

IndoStar has a built-in advantage when it comes to data backup: it uses the facilities of one of the firm’s investors, Everstone Capital, which is in the same building. “We can tap in to Everstone’s support system,” says Thapar. “It’s not the same disaster recovery a large bank would run,” he admits, but it helps save IndoStar some money. “This is a hybrid of doing it in-house.” Thapar retains some oversight responsibility for overseeing IT at Everstone, his former employer. “It’s not as secure as I would have wanted, but it makes sense at our size. To do this entirely on our own would be too expensive.”
LESSONS LEARNED FROM THOSE PROTECTING THEIR PASSION

1. **Hire an outside firm to maintain your security on a regular basis.** Many small businesses also contract with specialist firms to host their websites and email servers, run their firewalls, and manage all related security and software updates. Even if you would rather do it yourself, you should bring in a consultant to do a network security check to identify vulnerabilities.

2. **Limit access to sensitive data on your network.** Remove older data regularly and secure it.

3. **Use the cloud for backup.** This is a good option if space is an issue or in industries that have to keep records for years.

4. **Make sure company laptops used outside the office have the best security available in case they are lost or stolen.** Disable file sharing on computers used remotely, wherever practical. Tracking devices can also be added to mobile devices to make them easier to locate if lost or stolen. Encrypt all sensitive data.

5. **Create a virtual private network.** This can help protect company data when employees use laptops and mobile devices in hotels, airports, coffee shops and other Wi-Fi hotspots.

6. **Reinforce password safety.** Make sure everyone who can access your company network creates a password that is complex enough to defy an easy guess.

7. **Update software with all available patches.** It’s a simple, free and often overlooked safeguard. The majority of web-based attacks exploit the most common vulnerabilities and are thus totally preventable.

8. **Protect your money as well as your data.** Contact your financial institution and require verbal approval for any transactions over a certain amount. To prevent hackers from hitting your account with a series of small withdrawals, limit the amount of money that can be transferred from your bank account in a single day.

ACKNOWLEDGMENTS

Forbes Insights and Symantec would like to thank the following individuals for their time and expertise:

Richard Ashton, Co-Founder, Eiger Securities LLP, UK
Hisham Barakat, D.D.S., Vienna Smiles (a dental practice), U.S.A.
Jim Betland, President, Challenge Machine and Manufacturing, Inc., U.S.A.
Mois Cherem Arana, CEO, Enova, Mexico
Kevin Flanagan, Co-Owner, Custom Packaging Supply, Inc., U.S.A.
Kennelly He, IT Administrator, Millennium Institute of Sport & Health, New Zealand
Mukunda Krishnaswamy, Founder, Lumos Learning, U.S.A.
Peter Morrison, CEO, Bohemia Interactive Simulations, Czech Republic
Rasha Shehada, Executive Managing Director, Diamond Line F.Z.E., UAE
Pankaj Thapar, CFO and CTO, IndoStar Capital Finance Private Ltd., India
Matt Zurn, General Manager, Zurn Plumbing Service, Inc., U.S.A.
ABOUT
FORBES INSIGHTS

Forbes Insights is the strategic research and thought leadership practice of Forbes Media, publisher of Forbes magazine and Forbes.com, whose combined media properties reach nearly 50 million business decision makers worldwide on a monthly basis. Taking advantage of a proprietary database of senior-level executives in the Forbes community, Forbes Insights conducts research on a host of topics of interest to C-level executives, senior marketing professionals, small business owners and those who aspire to positions of leadership, as well as providing deep insights into issues and trends surrounding wealth creation and wealth management.

Bruce Rogers
CHIEF INSIGHTS OFFICER

Brenna Sniderman
SENIOR DIRECTOR

Kasia Moreno
EDITORIAL DIRECTOR

Brian McLeod
MANAGER, NORTH AMERICA

Lawrence Bowden
MANAGER, EMEA

Curtis Bergh
DEPUTY DIRECTOR, APAC

Deborah Orr
REPORT AUTHOR

Dianne Athey
DESIGNER