3.1 INTRODUCTION TO THE SMALL AND MEDIUM-SIZED ENTERPRISE (SME)

If a startup company manages to survive its first years, it then enters into the world of the small and medium-sized enterprise (SME). In doing so, it faces a very different set of cyber-related risks than it had to deal with in its earlier days. Internally, the SME lacks resources to protect itself properly against savvy and aggressive cybercriminals. Even more than the startup, the SME offers an increasingly tempting target to hackers on the search for vulnerable victims. In addition, the SME’s supply chain is different from when it was a younger firm. The university most likely plays a much more limited role now to the firm. In addition to the venture capitalist, the growing SME will increasingly have to start dealing with institutional investors, such as local banks. One of the more important considerations for the SME is putting in place a sophisticated IT system, one that can grow with the firm without requiring expensive revamping as the company passes through its various stages of expansion. More and more, SMEs rely on outside vendors to design, install, and maintain these systems. The advent of the “Cloud” is another option for IT services that has been attracting these smaller companies. Each of these actors—banks, IT vendors, the Cloud—exposes the SME to cyberthreats the likes of which it has not previously had to deal with. For the SME, the stakes are even higher, and the challenges no doubt greater, than before. This chapter considers these new threats and the challenges they pose for these firms.

3.1.1 The Nature of the SME

There is really no set definition for what is and is not an SME. Nevertheless, recent articles and studies address the nature of these companies and attempt to establish some criteria for what should be considered a legitimate SME. It is hardly necessary to state that SMEs vary in size and are active in all sectors of the economy, including services, manufacturing, transportation, farming, and...
many other areas. For the purposes of this book, we can agree that SMEs generally include any enterprise with 500 or fewer employees or with revenues of less than $25 million. Within this category, SMEs can be divided into three groups. Microenterprises employ fewer than 10 people and have annual revenues of less than $2 million. Clearly, these types of businesses may overlap with what we have termed startups or spinoffs. The next level brings us into the “small enterprise” sector, with each company employing fewer than 100 people and bringing in revenue of no more than $10 million. Finally, the medium-sized firms employ up to 500 personnel and have revenue not exceeding $25 million.

Whatever the size of the SME or the type of the activity with which it is involved, the species as a whole exhibits three major traits: it wields an inordinate amount of influence over national economies, it is a leading driver of a country’s innovative push, and it encompasses firms with one common problem: resource limitations. These will be discussed presently.

### 3.1.1.1 Economic Impact of SMEs
SMEs are a major force in the world’s economy and account for the vast majority of firms in the United States. Population growth is a major driver of the SME sector of the economy. As reported recently in a Forbes article:

> Population growth provides fundamental support for growth in the small business sector. With three million additions each year, the demand for services grows (more haircuts etc.) and this demand is to a large degree met by small businesses [1].

More than any other area of the US economy, SMEs are a major force in the US services sector. Around 80% of SME’s gross domestic product (GDP) contribution is in the services area, particularly the wholesale and retail sectors. They also contribute approximately one-third of the country’s total exports and thus are an important driver of the US trade surplus and the growth of balance of payments.

Given their significant role in US economic activity, it is to be expected that SMEs are a leading creator of jobs, accounting for about half of all positions in the American economy. These jobs boost the purchasing power of the American worker; through the multiplier effect, the income produced in the SMEs ripples through the economy as a whole, raising the profits of all companies, large and small.

### 3.1.1.2 Innovative Impact of SMEs
SMEs are major engines of innovative life in a country. The technological position of any country—and thus its ability to sustain healthy economic expansion—depends mightily on the growth in and nature of its SME sector.
Within the United States, we need only to tap the records of the Patent Office to get a sense of the pervasive presence and dynamic participation of the SME in the country’s innovative culture. Taking patents as the measure for innovative activity, SMEs generate a far greater number of patents per employee than do larger firms [2]. But even more importantly, the patents of SMEs tend to be more significant both technically and economically than those of the bigger firms [2]. SMEs are also far more efficient (by necessity, it can be argued) in creating these more important patents than the big companies: they use fewer R&D resources to produce more ground-breaking patents. As Richard Leifer and his colleagues tell us in their book *Radical Innovation: How Mature Companies Can Outsmart Upstarts*:

Small entrepreneurial firms are the source of most radical innovations... This widely held belief is supported by the success of entrepreneurial ventures in Silicon Valley ... and wherever else new companies with radical innovations sprout and take root. Think of the upstart firms that have pioneered the technologies and business models closely associated with the history of the Internet and e-commerce (America Online, Amazon.com, Yahoo!); personal computing (Intel, Microsoft, Dell); and biotechnology (Genentech, Biogen) [3].

But the innovative power of SMEs extends even further. In addition to directly turning out some of the most important modern technologies, they actually create a culture of innovation within society. They provide important opportunities for citizens in developing countries to experience entrepreneurial thinking and strategies that come with conceiving, building and operating their own businesses. And within the developed world, they bring this experience to a broader sector of society. SMEs have been a way for immigrants and minorities in the United States to advance economically while at the same time contributing to the economic growth of the country. Minority-owned businesses account for approximately one-fifth of all US firms and the majority of these, as might be expected, are SMEs [2]. These businesses extend globally, in part because of the remittances sent abroad that are generated by these enterprises. While many of these businesses tend to be in low-tech areas such as retailing and wholesaling, increasingly minorities and immigrants are helping to found and grow some of the most innovative companies in such areas as energy, IT, biotech, healthcare, and manufacturing. Silicon Valley is replete with such enterprises and SMEs are responsible for cultivating a dynamic innovative climate in other parts of the United States and in many regions of the world.³

³Israel, for example, has become a thriving place for highly innovative SMEs. Europe of course has created its own stomping grounds for high-tech companies, often centered around universities. For the role of SMEs as the driving force behind “other Silicon Valley” clusters around the world see [4].
3.1.1.3 SMEs and Resource Constraints

Despite their importance in the economic fabric of the US and their central role in fueling innovation, SMEs are tightly “resource-constrained.” More than large firms, SMEs face scarcities of financial and human inputs that impose severe limitations on their ability to bring new products and services to market and to take advantages of opportunities abroad (such as inability to meet quality standards, obtaining requisite knowledge of foreign markets, or forming relationships with local networks and government officials that could facilitate market entrance). SMEs certainly face greater disadvantages compared with their larger competitors. In addition to simply having smaller cash reserves at their disposal, their inability to achieve scale economies further restrains their growth and can threaten their very survival. Because they cannot make special bulk deals with suppliers, they are often faced with paying higher prices for goods sold and because of their relatively high unit costs, they cannot easily absorb regulatory and other business costs. In short, they cannot expect to match the profit margins of the big firms.

When it comes to innovation itself, while SMEs may be quite creative in conceiving new products and processes, they often falter badly when attempting to scale and commercialize their own technology. These activities typically require considerable capital in amounts that are not usually within the realm of the possible for smaller enterprises. It is for this reason that highly innovative SMEs often succumb to the temptation of agreeing to be acquired by larger organizations capable of supplying the cash, facilities, and personnel necessary to transform a laboratory device into a commercial product.

Resource constraints impose further problems upon the SME when it comes to defending themselves against cyberattacks. Simply put, they do not have the economic and technical wherewithal to create and sustain effective defenses against sophisticated and ever-evolving cyberattacks. This resource shortfall hobbles an SME’s ability to stave off the most aggressive invaders, leaving it exposed on many fronts to every sort of criminal incursions that can be inflicted on its computer system.

3.2 CYBERCRIME AND THE SME

The SME is especially susceptible to cyberattacks for many reasons. But, as Symantec’s executive Vice President Brian Burch tells us, possibly the most important of these is that they are very young and relatively poor—they have not had the chance to build up cash reserves to purchase the defense needed to ward off the more persistent and clever hackers [5].
We can certainly identify certain ways in which large firms have the advantage over SMEs. Most importantly, they generally have the resources to put into place a security system that is comprehensive and centralized. They often integrate network devices and equipment into one coherent system that makes it possible to rapidly identify and act upon immediate and unanticipated attacks. In contrast, SMEs, without the same level of resources at their disposal, cannot imbed this level of comprehensiveness into their network security. The prevalence of employees who work from home, which tends to be more of an issue with SMEs than with the more tightly structured larger corporation, exacerbates the problem by creating far-flung work centers that are more difficult to link into a tight, unified system. These semi-independent centers are even less secured than the computers that are on the SME’s physical site and so offer cybercriminals even more points of entry into the company’s network. These electronic devices used freely by employees are linked in numerous ways with the company’s computer system, which greatly adds to the danger that a cybercriminal could find his or her way into a company’s most sensitive records and accounts from the most innocent of entry points. In one recent case, employees in the back office of a small firm downloaded a pirated video game that happened to have malware attached to it. Since they were using an office computer as the video game console, the malware entered into the business’s most vital records, wreaking havoc on the company’s accounts and on its long-term reputation with clients [6]. In a similar way, in small companies, the Point of Sale (POS) system is often run on the same computer that is used to check company email. In such situations, employees clicking a malicious link or opening an infected attachment on that computer can give the hacker access to all customer information stored on that POS [7].

But restricted cash supply and an informal and decentralized organizational structure are just the tip of the iceberg of potential troubles facing the unsuspecting SME. Many of these firms specialize in one product or service and have a limited pool of clients. They do not have the luxury of multiple revenue streams from different businesses. If a cyberattack destroys—or temporarily cripples—their one source of revenue, they face the unhappy prospect of having to shut down their entire operation. In these cases, SMEs conduct business “on a knife edge” and without the comfort of a safety net to cushion the fall [8].

The SME not only contends with more sophisticated hackers but also with a digital world that is more difficult to manage. Since 2000, the amount of data that flows over the Internet has grown at a staggeringly fast rate. The rapid transition from a cash to a “cashless” society is, by some accounts, one of the major reasons for the flood of data that has plagues businesses. The SME simply cannot upgrade its computer capability to keep up with a world increasingly...
awash in digital information, and so it struggles to find ways to keep this data out of the hands of cyber thieves. As SMEs are slow to adapt to the this new reality and have gaping holes throughout their systems, hackers find them easy prey.①

Of course, the very fragility of SMEs makes them extremely tempting target sites. Since larger companies are increasingly “upping their ante against cybercrime” and spending their money on the best security they can get their hands on, this leaves SMEs that much more exposed. With the big organizations now less attractive due to their heightened defenses, cybercriminals have often had no choice but to go after the smaller fish, hoping to obtain useful data that might have strategic value or that they could sell on the black market [10].

Another dangerous situation that makes the SME the likely victim of hackers is the increasingly automated nature of cyberattacks. The weak defenses put up by SMEs makes the mass-attack model practiced by hackers that much more devastating. They can attempt to infiltrate a large number of SMEs in a relatively short time. Hackers may not then actually be targeting any one firm in particular, but “trying the locks” of many businesses to see which ones they can easily penetrate. Since the more secure defenses of a larger company will deter would-be hackers, they then opt for the far more vulnerable—and less troublesome—SMEs.

It is not difficult to imagine how vulnerable such SMEs are in the face of large-scale hacking attacks which, rather than target a specific company, scan a wide range of firms with the aim of locating and going after any vulnerable spots they can find, and siphoning off as much information as possible. No SME, with their many vulnerabilities, is safe under such indiscriminate assaults. And the greater speeds of computers—as microchips become smaller and more powerful—means that hackers can easily make many more hacking attempts in any day than they could just a few years ago. Not only can cybercriminals make assaults on many more targets than before but, once they do locate a victim, they find their way into its system and extract what they need much faster than ever before and often even before the SME, with its slower response time, even knows that it has been infiltrated.

Resource troubles, digital overload, narrow product range, computer speeds, and technical limitations are not the only causes of problems for SMEs. The simple fact that many of these firms are less well known compared to the bigger

①In a New York Times blog a few years ago the author identifies such forces as technology, investment, standards, and leadership—and the inability of SMEs achieving all these—as important factors in limiting the growth of small and medium-sized firms. While the article does not mention the cybercrime issue, this chapter argues that the cybercrime problem for SMEs spans all four areas and will continue to gain power as bottlenecks to growth in the years to come. See [9].
companies also works against them. Because so many of these enterprises are unpromoted to the point of near anonymity, hackers can attack without significant publicity—certainly less than if they were to directly hit a much larger corporation. This secrecy has its own rewards for the cybercriminal mind, not least of which is the ability of the perpetrator to hack into the firm’s computers without being detected for long periods of time, all the while collecting and siphoning off economically useful data and information [11]. In addition, since so many of these smaller companies are vendors to larger corporations (as will be discussed further in the next chapter), attacking them offers the enticing prospect for hackers to find their way past the forbidding fortifications put up by corporate IT by penetrating into the vendors’ networks and, from there, moving surreptitiously into the larger corporate computer system [11]. The logic here of course “…is that often, when going after manufacturing companies in the supply chain, hackers gain access to sensitive information of much larger companies” [12].

It is not a little ironic that the one attribute the SME appears to have that makes it highly competitive is also the one that attracts cybercriminals and thus exposes the SME to serious danger. The high degree of innovativeness enjoyed by this sector is the very same factor that entices hackers to go after these firms. A recent case shows how years of investment in proprietary research can be destroyed as a foreign competitor obtains the essential information by stealth. The company in question is a relatively small outfit that made an important component for an environmentally friendly product manufactured by a larger original equipment manufacturer. The criminals, who “maintained a close year-long presence in the company,” were able to steal “every engineering diagram, every piece of test data, even the marketing material for the product.” As a result of their successful efforts, the attackers were able to recreate the component and nudge the SME, which had spent its own resources on R&D, out of the market. A few weeks later, the same assailants hit another SME that made the other component for that same green product [13].

Finally, we cannot underestimate the problems that a firm’s own employees can cause because of their ignorance of how hackers work or simply not thinking before responding to electronic messages and prompts of various kinds. One of the main problems faced by SMEs is not spending time and money to vet potential employees—who might skim credit cards, for example, or simply do something wrong unknowingly. This means that SMEs are particularly susceptible to social engineering scams, such as fooling employees with seemingly legitimate emails that instruct them to transfer money from the business to the hackers’ account.

In going after SMEs, hackers secure specific and very effective tools to infiltrate the smaller companies. The so-called “ransomware” schemes lock computers
and then email a demand for a ransom fee that needs to be paid before the
attackers will release the computer system [10]. The average SME, being a
one-trick pony with all its revenue coming from one type of product or service,
is particularly vulnerable to this type of attack; if the firm does not surrender to
the terms of the hacker, the entire company’s ability to function is severely jeop-
dardized. In addition to ransomware, “malicious software” also effectively
achieves its goal of stealing information from mobile devices operated by
SME employees. The smaller operation is at a greater disadvantage than is
the larger company for two reasons: the pervasiveness in the use of mobile tech-
nology, and the lack of resources and time to closely monitor and secure these
devices from outside attack [10].

3.2.1 Indirect Costs to SMEs
The direct cost of a cyberattack against any firm, SME or otherwise, is usually
easy to pinpoint, namely the loss of cash, computer downtime, and tarnishing
of reputation. But there are indirect consequences as well and these may exceed—and significantly so—even the initial and more obvious initial dam-
ages. The SME faces its own particular and often highly damaging set of indirect
costs. There are a number of less obvious consequences of cybercrime that seri-
ously threaten SMEs’ ability to compete. One of the most important is their
increasing caution about trading online. While their reticence is understand-
able, avoiding the Internet means that they miss out on an extremely important
source of revenue and so lose a great deal of business over the long term. In such
cases, the SME is not the only victim. SMEs’ fear of engaging in cyber business
also damages the economy overall, given the very large role that such compa-
nies play in the commercial life of the nation [14].

Potentially even more harmful is the exposure that SMEs face when their
data and information are compromised by cyberattacks. In a type of “blame-
the-victim” scenario, SMEs compromised by clever hackers face legal and reg-
ulatory punishment for being targets, especially when it comes to the invasion
of financial accounts. Simply put, the laws that protect commercial banks are
not as rigorous as those that exist for personal accounts. This means that banks
are not always obligated to reimburse businesses when hackers successfully
siphon off money from SMEs’ bank accounts. This is especially true when
the bank can show that its security systems accord with federal guidelines
while those of the victimized business did not. In 2009, for example, hackers
stole nearly $600,000 from the bank account of Patco Construction, a small
firm located in Sanford, Maine. Not having a particularly sophisticated cyber-
security system in place, the company could not initially convince the bank to
cover the loss. (Patco eventually did get its money back from the bank, but
only after spending much time and money going after it in court.) [15]. There
are also additional and burdensome costs associated with money that has to be paid outright by victim SMEs to federal and state agencies. For example, the Federal Trade Commission (FTC) investigates and brings enforcement actions against companies it believes have ineffective security practices dealing with customer information. Significant costs come into play in defending such investigations. At the state level, the victimized SME is responsible for the cost in notifying customers who, in turn, can assert their own civil claims against the SME. Companies, for example, not compliant with Payment Card Industry (PCI) standards can be liable to substantial penalties and fines in case of credit card breach, and card associations could ban a company altogether from accepting cards—clearly a very severe blow to a retail SME [16].

3.3 CYBERCRIME AND THE SME SUPPLY CHAIN: WEB DESIGNERS AND THE CLOUD

SMEs operating within larger networks face additional problems above and beyond those already mentioned. The supply chain feeding into the typical SME is a potential source of digital contamination. As is the case with startups, SMEs rely on external sources of investment money, often in the form of venture capital (although it could also come from government sources, such as grants from federal and state small business development agencies). These funding sources often house sensitive financial, technical, and business-related information on their clients that can make them prime targets for hackers. Alternatively, cybercriminals who hack into venture capital (or government) networks may then clandestinely move into and infiltrate the SMEs who are their clients, causing even more damage to the latter, such as stealing customer information and invading internal accounts. The degree to which the network of the SME is integrated into that of venture capitalist or relevant government agency determines the likelihood that such unwanted intercourse takes place. Accordingly, the SME has to be very selective about the venture group and financial services company with whom it does business. It wants to avoid having its partners be the source of vulnerabilities to its own computer network. c

The very multitude and diversity of these entities means that it is very difficult—indeed, virtually impossible—to come up with general security standards and protocols for minimizing the risks of cyberattacks against SMEs. This lack of standardization in cyber risk management become all too clear when we consider the

---

cThe SME in fact, when possible, might attempt to pressure its vendors to meet rigorous security requirements before contracting their services. It might demand, for example, that the vendor provide strict, multi-layered authentication protocols to set up and access financial accounts. But in reality, SMEs have a challenging time in identifying much less implementing ways to manage the threat of cybercrime across the supply chain.
divergent interests and goals of SMEs as a whole. The most sensitive area of concern for SMEs within such high-tech fields as software development is the security of their intellectual property. This is certainly not the case for low-tech SMEs such as clothing retailers, who are more alert to securing the acquisition, storage, and transmission of its customer information [11]. Each small to mid-sized firm must therefore work with its own financial vendors to custom-design security systems and protocols. Such customization is time-consuming and often costly. Because time and money are two resources that SMEs do not typically have in abundance, these firms often skimp on this aspect of their business, thus leaving themselves wide open to the devastation of attack by cybercriminals. The dangers to SMEs from the outside via the supply chain arise not only from venture capitalist with which they do business, but, somewhat ironically, from the IT specialists they retain to set up, operate, and maintain their computer network and from the “Cloud” into which more and more SMEs entrust their most sensitive and confidential corporate information.

3.3.1 IT Vendors

More so than larger organizations, SMEs, lacking the resources to create their own IT functions in-house, are more likely to hire outside IT vendors to handle their Internet and web-based needs. This means that these suppliers of IT systems are primarily responsible for determining the degree to which an SME client is protected against cyberattacks. But, in fact, this dependence on external expertise places the SME in an extremely risky position, since such IT service suppliers can vary greatly in their experience, training, and resources.

3.3.1.1 The Functions of the IT and Website Consultant

IT and website consultants can be divided into four major functional specialties: website designers determine the layout, graphics, text, and navigation of the site; graphic designers create graphics, colors, and fonts; website developers take the design and write the code to implement it; and Internet marketers help increase traffic to a client’s site through search engine optimization. In the following discussion, we shall focus on the two most important of these: website designers and developers.

IT and website consultants are typically small outfits who do not have the luxury of being able to specialize; they often have to be ready to perform two or more of these various functions. This “jack of all trades, master of none” business model demands website consultants be flexible as needed but only within limits: without the focused specialization needed to custom-fit website security systems properly for the particular client requirements, the SME hiring this service will find itself vulnerable to the most sophisticated cyberattacks. In fact, many IT and website consultants simply do not—or cannot—provide adequate data protection for the SMEs with which they do business.
3.3.1.2 The IT and Website Consultant as Perpetrator

IT vendor mismanagement is one of the most serious vulnerabilities facing small and medium-sized companies. In some cases, the hired firm itself is unscrupulous and so becomes the very source of the problem. A case in point occurred in 2013, involving a stolen identity. A small firm engaged a web developer who was recommended by a friend of the SME’s owner. The developer set up a system with specific instructions to the owner never to turn off the computer, explaining that this allows continuous flow of software updates. In actual fact, keeping the computer on made it easy for the web developer to steal the owner’s IP address and, in turn, to impersonate her online. The owner and her business were now “naked and exposed” to data theft and manipulation by the larcenous vendor. The latter quickly began to host the company’s personal and corporate email accounts on his servers, set up social media accounts in her name, and steal sensitive personal information from her. Soon, he began blackmailing her, threatening to destroy her company by posting publicly on her website lies that she was a debtor with whom no one should do business. This nightmare scenario became only too real for this new business, a situation intensified by the lack of laws or regulations to help protect her against such abuse:

An Internet service provider and website developer... is trusted to an alarming degree ... there are no safeguards in place to protect small businesses against their web/internet provider, other than their rights as citizens under the consumer protection act... In the absence of regulations the perpetrator can misuse his knowledge at any time [with the belief] he can cover his tracks, and evidence [17].

3.3.1.3 The Limitations Placed on the IT and Website Consultant

As noted, IT and website consultants tend to be small businesses themselves, many in fact qualifying as microbusinesses (with fewer than 10 employees). As with many types of SMEs, these outfits have precious few resources themselves and time management is a persistent problem. Even if they are not dishonest and out to steal identities or blackmail their clients—and most are emphatically not—they simply do not have the wherewithal to offer their clients the level of protection needed to deflect sophisticated and persistent cyberattacks.

Even if an SME can vouch for the integrity of an IT vendor, it stands to reason that there are still compelling reasons for the small or medium-sized customer to be very wary of the web developers/designers with whom they deal. The micro-sized nature of the vendors’ companies means that they may have very little time that they can actually spend on the particular problems and needs of every client. They must devote a large proportion of their efforts on just finding new clients in order to keep cash flowing. With only a few people working in
many of these businesses, they are not likely to have on their staff specialists who can cater to the unique demands of every SME that engages them. The quality of the vendor can also not be taken for granted. The industry is still regarded as a sort of high-tech “wild west,” possessing all of the aggressiveness, creativity, risk-taking, and “winging it” mentality that this implies. There are no industry standards with which to gauge the quality of a website consultant. Also important is the fact that barriers for entry are rather low. All that is needed is some modest startup money (often less than $30,000) and certain web design skills, which can be self-taught [18]. Nor is it true that only the best in their field can survive. According to one veteran of the industry, it is usually not too difficult for even the less competent outfits to thrive for a while. New web design companies can generally find work fairly quickly. While these first projects tend to be small and low paying, they allow the new operation to start bringing in revenue. Certainly, the less gifted of the companies will often die a quick death, but even the less-than-stellar performers can find enough work to keep going and indeed begin to grow as they net themselves the more desperate clients who need immediate IT help.

3.3.1.4 The Problems of Specialization and Global Competition

Survival does not by any means point to competence, at least as concerns the specific needs of SMEs. As discussed, each type of small and medium-sized firm calls for its own specific requirements. Thus many—if not most—web developers may attempt to approximate but in the end cannot provide the expertise needed to deal with the increasingly sophisticated threat of the 21st-century hacker. In stark contrast to the software development business, web development and design firms do not generally offer customized services. Seldom concentrating on dedicated applications, these small operations take whatever jobs they can; economies of specialization, which can prove such a powerfully effective force in addressing the distinctive security requirements of each SME client, do not have a chance to take root in this sort of generalized climate. While website consultants may be able to adjust their talents satisfactorily to a wide range of problems, they are not necessarily able to handle the more intricate demands unique to a particular company. Certainly, the returns for website consultants are not sufficiently intriguing to justify the time and effort that goes into realizing such specialization. As one web designer complains:

Like everyone else, we charged clients fixed rates. If our projects were a storming success, our reward remained the same. At best, you’ll earn yourself more work. Well done! You... essentially earned yourself more, slightly better work [18].

The surge of globalization also continues to crank up the pressure on web developers and designers. Larger firms—as well as a growing number of SMEs—
depend more and more on offshoring their IT and website needs. Leaving aside the issue that relying on such services from abroad increases the risks of cyber-attacks on US businesses through the foreign vendors, there is the problem that outsourcing to foreign countries forces US-based vendors to compete against the much lower prices charged by skilled web designers working in developing countries:

One reason why web development is a dead industry is because of outsourcing. I can now hire some Indian guy that lives in the village where he doesn’t have rent and much bills to pay and never have to worry about government regulations and tax. Why would I hire and pay you $500 if I can pay him $5 [18].

The intensification of global competition in IT consulting puts further pressure on domestic vendors to cut corners and to contract jobs for which they may be ill qualified.

It may seem at first glance that SMEs have a greater chance of finding more experienced, specialized, and reliable IT and website vendors in large cities where there should be more options of suppliers from which to choose. However, this is not necessarily the case, for a wealth of opportunities also exist for the vendors themselves, and this means that even the less proficient ones can do quite well. Financial opportunities do not just attract the best in the business; they lure in just about anyone with a computer and a modicum of skills and an attractive presentation. Cities also offer vendors a level of anonymity that allows them the unfortunate freedom to antagonize existing customers with sub-par performance and then to move on to new and unsuspecting market opportunities. Due to the lack of “connectedness” that is such an integral part of the urban landscape, poor performers can shake off past failures and apply dynamic marketing strategies that attractively package potent but empty promises that capture the business of unwary victims. In the cold hustle and bustle of the cities, the Salieris of web development can thrive at least as well as the Mozarts.

3.3.1.5 The Open Source Problem: The Case of “WordPress”

As SMEs themselves, and often not much more than mom-and-pop enterprises, IT and website consultants find ways to reduce the costs and time which they spend conducting their business for each client. Working efficiently and as lean as possible is crucial for survival, at least in the short term. As noted, there is no time and certainly few resources for such companies to spend on particularized, bespoke projects. Generally available, relatively inexpensive, and (more or less) standardized technology is exploited on any and all projects whenever possible. But there are serious drawbacks in depending too rigorously on such “off-the-shelf” strategies when dealing with a wide
variety of clients with very different IT and website design needs, as the following case demonstrates.\textsuperscript{d}

In 2015, cybercriminals hacked into numerous websites across North America. Many of these were small or medium-sized businesses, such as a Montana credit union (Southwest Montana Community Federal Credit Union in Anaconda, Montana). Happily, no actual data breach occurred, only “a simple injection of graphics” onto companies’ web pages. Essentially, the attack was of a low level and involved the placement of web graffiti.

However, this incident was still very concerning for the credit union—and other SMEs—because it dramatically demonstrated how vulnerable their systems are to future attacks. The one common link between the hacked sites was that they all used the same, standard platform known as WordPress. WordPress is an open-source platform that is the most popular blogging system in use on the Web today; nearly a quarter of the world’s websites are built on it. However, being so well known as the standard “go-to” blogging platform has its disadvantages; cybercriminals know how it works and, from this knowledge, have learned that the platform has a serious weakness: easy access since the system is densely populated with thousands of third-party “plug-ins.” These cause WordPress to be extremely vulnerable, with hundreds of thousands of web-based attacks executed every year. The perpetrators that infiltrated the Montana credit union found their way into the platform via a particular plug-in called “Fancybox.”

Many small banks and credit unions use WordPress as their host because it is free, with no licensing costs. The problem with this, however, is that these banks and credit unions will use 20–30 different plug-ins that are all written by different people. This means that not all plug-ins have had the proper security measures applied for specific systems to prevent potential threats. Also, plug-ins are not regularly updated to prevent hacking. Therefore, any one of these plug-ins offers a possible route of entry for cybercriminals. This rather scary situation leaves many banks vulnerable to future data breaches. Starting in 2007, WordPress websites started experiencing attacks. By Jun. 2013, 70\% of e-commerce plugins were vulnerable to hackers, who could upload their own files and malware to collect sensitive information without being detected for long periods. This placed many companies, including numerous SMEs, at risk. While web designers and developers can use special tools to analyze potential vulnerabilities, there are problems: not all vulnerabilities can be detected by this technology and these tools take time and money, two things that many web developers do not have.

The problems experienced by free and open systems such as these “strikes at the core of web development” and is often missed when such functions are outsourced by SMEs; so many web development firms simply do not have the time,

\textsuperscript{d}For background on WordPress and on this particular case study, see the following [19, 20].
money, or expertise to ensure that such gaps are plugged tight. Thus, outsourcing web development work on the assumption that it is secure is a risky proposition. Additional steps have to be taken; updates and other modifications to the mass-produced software are needed, and these can easily be missed by web developers and designers who are dangerously busy trying to make ends meet in their struggling, resource-challenged businesses.

### 3.3.2 The Cloud

Administrators of the Cloud, within which SMEs often do business, can certainly be considered a type of IT vendor. Yet the Cloud is very different from the small operations discussed in the previous section. Rather than designing and installing website functions for individual companies, purveyors of Cloud services create, operate, and maintain an overarching, all-purpose system capable of absorbing and running the websites of many companies simultaneously. Client companies pay for this service and gain access into their particular accounts through unique codes. But more than this, the Cloud is a kind of Internet-based computing network that provides services allowing different individuals and companies to jointly access a shared pool of data and information. Using Cloud computing, individuals and companies do not have to store and call up information on their own systems, but rather can do so at any time (on-demand) by going on the Internet, finding their third-party Cloud service provider, and providing the appropriate login numbers. For example, when you take a picture on your smartphone, it is stored on your phone’s internal memory drive; if the phone itself is destroyed, so is that picture. However, when you upload the photo to Instagram, you are uploading it to the Cloud; if you lose your phone, the picture remains intact in the Cloud to be retrieved using any other appropriate computing device. To take another high-profile case, Adobe recently moved its creative services to the Cloud. Customers can no longer buy the Creative Suite (Photoshop, InDesign, etc.) in a box set. Instead, they pay a monthly subscription fee to use each individual service. This sharing of resources enables users to enjoy an economy of scale advantage in their operations that they could not acquire alone. In this sense, Cloud computing resembles, and is often compared to, a utility’s electricity grid.

Cloud computing is a highly desired service due to the advantages of centralized, high computing power, cheap cost of services, performance, scalability, and full-time accessibility. In response to expanding demand, companies, including such major high-tech players as Amazon, IBM, and Oracle, have introduced their own versions of the Cloud. While some Cloud vendors experience growth rates of over 50% per year, Cloud computing is still a young industry that faces its share

---

*eThe Cloud can be considered a vendor/supplier to SMEs (or any company) using its services. At the same time, as we shall see, it is a very different sort of service from the mom-and-pop IT consultant we have just been discussing.*
of problems, including the need to make the service more reliable and easier to use. Nevertheless, the advantages of Cloud computing remain compelling to many types of individuals and a variety of companies. By switching from company-owned hardware and software to “per-useservice-based” models, individuals and companies avoid the high costs of purchasing, operating, and maintaining high-cost IT assets, and can instead focus their time and resources on their central, core business.

3.3.2.1 SMEs and the Cloud
Many SMEs consider the benefits offered by the Cloud to be highly enticing. They are particularly intrigued by the possibility of doing away with the need to buy, install, and maintain a complete IT infrastructure. All that is required for full IT and website ability is dedicated Internet access to the Cloud service. They believe that renting third-party Cloud services in lieu of laying out cash in setting up one’s own system in-house—reducing the need for expensive web servers and large and skilled IT teams—must result in higher operating efficiencies and greater profit margins [8]. Those who champion the Cloud for SMEs point as well to the enhanced visibility of data and of the potential for collaboration. Cloud-based accounting systems, for example, render a business’s finances easy to see and review by all of the most important parties at any time. This ease of inter-departmental (and even inter-company) collaboration helps to break down barriers between a company’s operational departments and thus greatly streamlines and accelerates the decision-making process. The surge in the use of mobile devices (laptop, tablet, smartphone) and the consequent rise in work being done away from an SME’s physical premises make the Cloud even more relevant in an SME’s strategic planning and goals to streamline and seamlessly integrate accounting, billing, and inventory functions, thus propelling efficiency, productivity, and performance within the SME.

3.3.2.2 Three Big Problems of the Cloud for SMEs: Specialization, Connectivity, and Shared Space
But securing data privacy and protection from cyberattacks is another matter, as “sensitive company data could be left vulnerable to a breach” [8]. The three-pronged problem of SME—specialization requirements, network connectivity issues, and the risks in shared data—erode the ability of “Clouded” SMEs to resist the onslaught of determined, skilled, and increasingly Cloud-savvy cybercriminals. The demand of SMEs for highly focused IT functions is of enormous concern. Critics of the Cloud contend that the IT requirements of SMEs as a whole are so dizzyingly varied and, with respect to individual companies, so highly focused, that they are beyond the capabilities of the Cloud’s overarching, one-size-fits-all structure to satisfy. They argue that the small or medium-sized firm is better off avoiding both the enchantments of the Cloud and the lure of
unreliable IT vendors altogether, and should instead bite the bullet and pay more for dedicated in-house IT staff.

Another big worry for SMEs who wish to embrace the Cloud is connectivity. Broadband communications is vital for companies to access and productively use the Cloud. This is something they have far more trouble controlling than larger companies. The latter generally have the resources to compensate for inadequate local broadband services, possibly by contracting high-bandwidth with a number of providers. But many SMEs simply cannot afford to take this rather expensive route. Their only option then is to use a single digital subscriber line (DSL) line, at least until fiber optics communications are available locally [21].

In addition to the issues of specialization and connectivity there is the problem of shared space. The fact that data and information for a company is stored in a “common space,” as it were, should give SMEs serious pause. Trust is a major concern when it comes to the ability of Cloud service providers to protect SMEs from piracy and other forms of cyber aggression. SMEs express concern that placing vital statistics such as financial details and employee information on the Cloud sets their firms up to become a victim of cyber theft by sophisticated hackers. This is particularly the case when corporate payroll files are placed on the Cloud for the purpose of managing cash-flow operations by way of checks, wire and fund transfers.

3.3.2.3 A New Business Model and the Benefits of the Cloud for SMEs

Such concerns do not deter those who champion the use of the Cloud as an important tool for SMEs. While they admit that the problems of specialization and the sharing of data and information need to be addressed, they aver that the benefits of the Cloud far outweigh its problems, especially when dealing with companies with severe resource constraints. The capital savings that comes with entering the Cloud has already been mentioned. Even if an SME manages to secure its own in-house IT system, the dangers of costly computer breakdown are always lurking. SMEs are particularly susceptible to computer failures of one sort or another. Lack of resources is one reason for this: they often do not have the cash or the personnel to keep the company’s computers and network up to date technologically, which increases the risk of malfunctions. And of course, as discussed earlier, SMEs are a prime target for cyberattacks and the destruction of IT equipment and services within the company. The Cloud, many claim, is the proper way to manage such risks, for even if hackers manage to infiltrate your Cloud account, you have no risk of your own physical plant being corrupted. Moreover, it is believed, the Cloud greatly eases the process of scaling IT requirements as the firm grows. As SMEs expand their operations, these also need to grow with the company. The Cloud allows that to happen without requiring complete overhauls every time a firm reaches a certain size (just as
a child’s clothing needs replacing as he or she grows). The Cloud can be particularly valuable in this regard in that it—and not the SME—takes on the responsibility of expanding needed bandwidth and data capacity for companies as they get bigger. As one advocate of Cloud services for small and medium-sized businesses says:

[SMEs] don’t want to manage that [in-house] equipment any more, it’s just too intensive from a resource perspective and from a monetary perspective, and it’s inflexible, as it won’t adapt itself to companies during a time of expansion. With an on-demand[Cloud-based] infrastructure you can start with what you need today without worrying about tomorrow or the day after because the cloud can scale with you as and when needed [22].

What’s more, proponents of cloud technology believe that the innovative “on-demand” business model of the cloud actually does permit SMEs to meet their highly specialized needs, certainly to a much greater degree than critics often allow. In fact, they allege, what makes cloud computing so powerful a technology is that it tells businesses that they can look well beyond their immediate facilities—those four walls—in thinking about and implementing data management systems. The firm itself does not have to commit major capital to complex and expensive systems—both hardware and software—and spend the time and resources worrying about regularly maintaining the technology in top-notch condition. And even if the company does this, upgrades often mean tearing down the old and installing a whole new IT complex. This is not a winning prospect for SMEs. The Cloud takes advantage of economies of specialization and offers SMEs the ability to shop around for just those services they need at any particular moment. When these needs change—and when upgrades in existing services are called for—the SME can simply search for an appropriate service from a number of competing providers and so realign itself with another, more advanced system offering best-practice solutions through a new service contract. Rather than passively expecting a business to tell the IT industry what it wants and then wait some more for the industry to create it and put it into place—a process that can be both lengthy and expensive—the Cloud designs its own vision of what such services should be and what they should provide, and then offers these technologies to companies who pick them out from a catalog of possible technologies with on-demand and just-in-time speed and efficiency such that “IT organizations can manage the entire service lifecycle, from managing customer demand to ensuring service-level compliance and from driving process efficiencies to tracking costs” [23]. In this sort of business model, a company’s IT department, no matter how small, can leverage the resources of the Cloud to arrange a first-class IT system for the firm. In this way, IT activity within the SME does not have to be a money pit, sucking resources from the company with little to spare in a futile attempt to stay current with the latest technology that only larger firms can comfortably afford. Rather, the SME’s
computer center can more profitably play the role of the service broker, "sourcing services from outside" as the various departments require.

The Cloud does more than save the SME money; it also helps revenue to grow. It reduces time to market, an ability that is essential in retaining current customers and extremely useful in persuading new ones to choose the SME over larger competitors. As one executive observes: “it prevents those competitors from becoming stronger and therefore enhances the SME’s competitive strength in the market. Furthermore, IT organizations help SMEs to stay nimble as IT services can be provisioned in a timely way, on-demand, and with the illusion of unlimited capacity” [23].

### 3.3.2.4 The Outsourcing Question and Difficulties in Protecting Client Accounts

Both the champions and critics of the Cloud can argue these points ad nauseam and still not come up with a definitive answer as to whether the SME enjoys net benefits or suffers net losses by using the Cloud and its services. Despite all the expectations and the media and industry hype of the Cloud, especially as a solution to many of the resource restrictions and competitive problems faced by SMEs, the question of whether it offers SMEs the digital security they require continues to be the hot-button issue in the land of the small and medium-sized business. The following list of questions that, according to skeptics, SMEs need to ask hammers home the security issues facing an SME contemplating becoming a client of the Cloud:

- Is the Cloud service provider operating a legitimate business that is in it for the long haul? What if the Cloud service provider goes out of business or is acquired by another company? Will data remain available after such an event?
- In this context, what if IT organizations decide to decommission the Cloud services? How will data be transferred from the Cloud service provider back in-house or to another service provider? Who has access to sensitive data?
- What are the personnel’s qualifications and how does oversight of privileged personnel work? Where does the SME’s data physically reside? Is the location of data something that is of importance? Are there specific jurisdictions that are preferred for data location or that have to be avoided?
- How about regulatory compliance? SMEs are responsible for security and data integrity, but are the Cloud providers willing to undergo external audits and certifications? Is data being segregated appropriately? [23].

Even if an SME can answer these questions to its satisfaction—and leaving the issues of specialization, connectivity, and shared digital space for the moment—the reality is that it is quite difficult practically for a Cloud provider to protect a client adequately, for two main reasons. First, internal glitches within the SME itself can—and often do—jeopardize the integrity of that client’s Cloud account. In-house vulnerabilities exist within the company because of the
growing sophistication of cyberattacks that make effective use of social engineering. For instance, stealing sensitive information can be accomplished through targeted attacks, such as spear phishing. Even less sophisticated means, such as telephoning the company disguised as a worker who needs to remotely get the login credentials for the company’s account on the Cloud, can be extremely effective. By such low-tech means, staff can easily be manipulated into leaking proprietary and extremely sensitive information that will unlock the door to the company’s Cloud account for the hacker, at which point “you might as well kiss your data and your reputation goodbye” [24]. Then, too, there is no way that a Cloud provider can offer effective protection for all clients. Entrance can be made from anywhere in the world at any time. Even more, in the majority of cases, service in the Cloud is provided through a browser, which is notoriously easy to crack. Cloud providers generally are not very effective even in just detecting an attack, much less preventing it.

SMEs that expect the Cloud to protect them, then, are hoping that it will provide that function. But in fact, it can only do so much; the rest—the most important part of the mission to protect data—must come from the firm itself. Veteran ethical hacker Peter Wood recently made that argument in a presentation at Data Centre World in London:

What’s different in cloud from a security view is when you’re renting software-as-a-service, you’ve given away the management of security to a third party… Do you want to outsource the responsibility for security? You can’t outsource the responsibility; you can only outsource the function. That doesn’t mean security can be ignored, because in the end it’s your brand and your reputation that’s on the line if there’s a data breach [24].

It is little wonder, then, that cybercriminals stalk Cloud accounts at a frighteningly rapid rate. This is not in the least bit surprising, considering the amount of important information that they could potentially exploit in a single attack. Such aspects of a company’s operations, including financials, production schedules, strategic directions, internal dynamics, personnel histories, and intellectual property, can all be found on the Cloud, and not just for one company but for many client firms. This virtual treasure trove of valuable intelligence concentrated in one place is irresistibly enticing to aggressive and clever hackers. They will do everything in their power to break into and exploit this “dazzling vision of superabundant swag.”f It’s not just that they succumb to some variant of gold fever—in the form of knowledge and information—there is a rational and understandable economic dynamic that operates: increasing their profits through economies of scale. As a recent report issued by Alert Logic Cloud Security explains:

---

fI am respectfully borrowing this colorful and beautifully descriptive phrase from Simon Schama’s history of the Dutch Republic [25].
Hackers, like everyone else, have a limited amount of time to complete their job... They want to invest their time and resources into attacks that will bear the most fruit: businesses using cloud environments are largely considered that fruit-bearing jackpot... Attackers are seeing this trend as well and are making concerted efforts to infiltrate businesses making use of cloud environments, just as they previously did with physical data centres [26].

These attacks have been growing very robustly. Alert Logic reported that, in 2014 alone, more than 3000 of its clients experienced numerous cyberattacks; this represents over 800,000 separate hacking incidents attempted against company files stored on Alert’s Cloud network. Even more ominously, a recent cyber virus called Venom made it fairly easy for hackers to invade and control a wide swath of Cloud-based data centers, including those of Amazon, Rackspace, and Oracle. The laser-like focus of hackers specializing in invading the Cloud is taking its toll in stolen data and information, for “Unlike in the past when hackers primarily worked alone using ‘smash-n-grab’ techniques, today’s attackers work in groups, each member bringing his or her own expertise to the team... With highly skilled players in place, these groups approach infiltration in a much more regimented way, following a defined process that enables them to evade detection and achieve their ultimate goal: turning sensitive, valuable data into profits” [27].

The cyberthreats against SMEs are very different from those that loom over the startup and spinoff. Internally, of course, both types of firms have to face the prospect of human error and ignorance—as well as the malicious acts of disgruntled employees—as potential weak links that might open the company to hackers.

**FIG. 3.1** SMEs: cyberthreats and the supply chain.
Externally, the dangers from the supply chain are somewhat different for the SME. Certainly, both startups/spinoffs and small and medium-sized businesses access outside investment companies. However, while the former are more likely to make use of angel investors and the smaller venture capital businesses, the latter receive their investment money from larger, more established venture groups and (as the SME grows) from institutional investors. In all of these cases, the trajectory of the cyber risk is a two-way path: the digital infiltration of the one threatens the other.

A major change as the startup/spinoff morphs into the SME is the weakening bond—and therefore fading cyber risk—between the firm and the university. In the place of the academy are IT vendors and the Cloud. The dominant path of risk here is one way: from these two providers into the company into which they feed. On top of these dangers, of course, hackers are not sheepish about launching a direct attack on the SME itself, for so many of these smaller shops lack the resources and technological wherewithal to ward off a frontal assault from more sophisticated and very determined cybercriminals. Fig. 3.1 shows these various sorts of risks faced by the SME and its supply chain.

As the SME grows into a larger, more mature firm, both its internal structure and its supply chain undergo further transformation forcing another shift in the risk-patterns of cybercrime. Now, the would-be hacker and the corporate executive must face one another across very different and in many way a more subtle landscape than when the firm had been smaller and resource constraint its biggest problem. The challenges, especially for the company, are different now and in many ways even more daunting despite the larger amounts of cash and personnel at management’s disposal. The next chapter visits this world of cybercrime and the large corporation.

References


